UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema

SISTEMA DE COMUNICACIÓN Y VIDEO VIGILANCIA BASADO EN TÚNELES VPN PARA LA INTEGRACIÓN DE LAS SUCURSALES DE LA COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES DE TUNGURAHUA EN EL ECUADOR

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Electrónica y Comunicaciones.

ÁREA: Comunicaciones

LÍNEA DE INVESTIGACIÓN: Tecnología de la Información y Sistemas de Control

AUTOR: Tuza Cuji Walter Isaac

TUTOR: Ing. Mg. Geovanni Brito Moncayo

Ambato – Ecuador

agosto - 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: SISTEMA DE COMUNICACIÓN Y VIDEO VIGILANCIA BASADO EN TÚNELES VPN PARA LA INTEGRACIÓN DE LAS SUCURSALES DE LA COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES DE TUNGURAHUA EN EL ECUADOR, desarrollado bajo la modalidad Proyecto de Investigación por el señor Walter Isaac Tuza Cuji, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que elestudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, deacuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de TercerNivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, agosto 2023.

Ing. Mg. Geovanni Brito M.

TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado SISTEMA DE COMUNICACIÓN Y VIDEO VIGILANCIA BASADO EN TÚNELES VPN PARA LA INTEGRACIÓN DE LAS SUCURSALES DE LA COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES DE TUNGURAHUA EN EL ECUADOR, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2023

Tuza Cuji Walter Isaac
CC: 185026635-2
AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, agosto 2023

Tuza Cuji Walter Isaac
CC: 185026635-2
AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Walter Isaac Tuza Cuji, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SISTEMA DE COMUNICACIÓN Y VIDEO VIGILANCIA BASADO EN TÚNELES VPN PARA LA INTEGRACIÓN DE LAS SUCURSALES DE LA COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES DE TUNGURAHUA EN EL ECUADOR, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, agosto 2023.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
ANDREA PATRICIA SANCHEZ ZUMBA

Ing. Mg. Andrea Patricia Sánchez

PROFESOR CALIFICADOR

Firmado electrónicamente por:
SANTIAGO MAURICIO ALTAMIRANO MELENDEZ

Ing. Mg. Santiago Mauricio Altamirano

PROFESOR CALIFICADOR

DEDICATORIA

Este trabajo va dedicado a mis padres Manuel Tusa y María Cuji, quienes con todo su cariño y amor siempre me estaban motivando e impulsando a seguir adelante y no rendirme en los momentos difíciles y de dificultad.

A mis hermanos, por el apoyo mutuo que nos tenemos, por los consejos que siempre me brindaban para no rendirme y seguir adelante.

A mi tío Vicente Cuji, que en paz descanse un agradecimiento enorme por todo su apoyo, por el tiempo compartido, por siempre motivarme a no rendirme.

A toda mi familia que siempre estuvieron pendientes de mí y de mi desempeño a lo largo de mi carrera, dándome sus mejores deseos a la distancia y apoyándome en todo momento.

Tuza Cuji Walter Isaac

AGRADECIMIENTO

Agradezco primeramente a Dios por siempre cuidar de mí y guiarme a cada momento en las decisiones que he tomado para cumplir cada uno de mis objetivos y darme la fortaleza en los momentos más difíciles de mi vida.

A mis padres por todo el esfuerzo que realizaron para dame una buena educación, que siempre supieron guiarme por el camino del bien apoyándome en cada tropiezo, gracias por el apoyo incondicional a lo largo de toda mi carrera.

A mis hermanos Iván, Víctor y Bertha por nunca dejarme solo, por ser un ejemplo de luchar por los sueños, por los consejos, por el tiempo y la ayuda que siempre me han brindado. Sin su apoyo, sin sus palabras de aliento este sueño no habría sido posible cumplir.

A mis amigos, más que una amistad formamos una hermandad, por el apoyo mutuo, por la ayuda que siempre nos brindamos, por los consejos y sueños que cada uno de nosotros tuvimos.

A mi tutor, Ing. Geovanni Brito por orientar y guiar durante todo el proceso del proyecto.

Tuza Cuji Walter Isaac

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente proyecto se basa en implementar un sistema de comunicación y videovigilancia utilizando redes VPN (Red Privada Virtual) para integrar las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en Ecuador, mediante estas redes VPN se procede establecer un canal seguro de comunicación y transmisión de datos empleando tecnologías de la información.

La instalación de este sistema de control mediante una red VPN tiene como propósito garantizar la seguridad de los usuarios de la Cooperativa, permitir la integración de servicios como telefonía IP y videovigilancia, estableciendo un canal privado de comunicación seguro entre dos puntos. Para ello, se aplican protocolos de comunicación sobre IP, encapsulamiento y cifrado de datos.

El proyecto se enfoca principalmente en brindar seguridad, confiabilidad y accesibilidad a la Cooperativa, implementando una sala de monitoreo en la oficina central de cada una de las sucursales, además de contar con un sistema de comunicación VoIP privado. Esto posibilita brindar diversas aplicaciones, como video llamadas, llamadas directas y conferencias de video en grupo.

Palabras Clave: VPN, Telefonía IP, videovigilancia, encapsulamiento, cifrado.

ABSTRACT

This project is based on implementing a communication and video surveillance system using VPN (Virtual Private Network) networks to integrate the branches of the Cooperativa de Ahorro y Crédito Vencedores de Tungurahua in Ecuador, using these VPN networks to establish a secure communication and data transmission channel using information technology.

The purpose of installing this control system through a VPN network is to guarantee the security of the Cooperative's users, allow the integration of services such as IP telephony and video surveillance, establishing a secure private communication channel between two points. For this purpose, communication protocols over IP, encapsulation and data encryption are applied.

The project focuses mainly on providing security, reliability and accessibility to the Cooperative, implementing a monitoring room in the central office of each of the branches, in addition to a private VoIP communication system. This makes it possible to provide various applications, such as video calls, direct calls and group video conferences.

Keywords: VPN, IP Telephony, encapsulation, encryption.

INTRODUCCIÓN

A nivel mundial las empresas buscan expandir sus sucursales o productos a diferentes ciudades del mundo, por lo cual necesitan tener una comunicación y vigilancia con cada una de ellas, de manera que esto es posible creando túneles VPN. Estos túneles VPN permite crear un canal privado de comunicación entre dos puntos de forma segura, esto se puede conseguir mediante la aplicación de distintos protocolos de comunicación sobre IP, encapsulación y cifrado de datos. Cuando se implementa una VPN se tiene varias ventajas como confidencialidad de los datos, seguridad y costo [1] [2].

En los últimos años el servicio de conexión a internet ha tenido un crecimiento de tipo exponencial y una considerable reducción en sus costos, ofreciendo mejores velocidades tanto en carga como descarga, es por ello que las empresas que prestan servicios de ISP propicia a la interconexión de redes LAN a través de VPN mediante el uso de internet pudiendo compartir servicios entre establecimientos situados en diferentes ciudades, incluyendo la posibilidad de conectarse y ser controlados mediante este [3].

En la actualidad, en Ecuador se evidencia un marcado aumento en el crecimiento de diversas instituciones, tanto públicas como privadas. Este crecimiento ha generado la necesidad de establecer nuevas redes que prioricen la comunicación total y parcial entre ellas, con el objetivo de contar con una transmisión de información rápida y segura. En consecuencia, cada una de estas instituciones invierte principalmente en equipos tecnológicos que permiten el transporte de datos e información de manera segura.

La Cooperativa de Ahorro y Crédito Vencedores de Tungurahua es una institución financiera que necesita conectar sus sucursales ubicadas en diversas ciudades de Ecuador. El objetivo es contar con una sala de monitoreo en la oficina principal de cada sucursal, así como tener un sistema de comunicación VoIP privado que permita utilizar aplicaciones como videollamadas, llamadas directas y conferencias con múltiples participantes. Para lograr esto, es necesario implementar túneles VPN mediante diferentes protocolos que garanticen la transmisión de datos de manera segura.

CAPÍTULO I

MARCO TEÓRICO

1.1 Tema de Investigación

"Sistema de comunicación y video vigilancia basado en túneles VPN para la integración de las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en el Ecuador"

1.2 Antecedentes Investigativos

Para el presente proyecto se realizó una investigación en repositorios de diferentes universidades, revistas y artículos científicos encontrando información importante que permite al desarrollo del tema relacionado sistema de comunicación para la integración de las sucursales.

En junio del 2021, en la Universidad Técnica de Ambato, Ecuador, Jessica Daniela Miranda Quishpe, en su investigación, "Sistema de comunicación en tiempo real con QoS para la integración de las unidades de salud de la provincia de Pastaza", señala que este sistema conecta 6 sitios diferentes ubicados en diferentes ciudades utilizando internet. Para lo cual utilizó Routers Mikrotik, que permiten la creación de redes VPN utilizando el protocolo IPsec, con las redes VPN crea una aplicación que permite compartir datos, voz y video entre las diferentes casas de salud. Estas redes ofrecen una confiabilidad de datos utilizando el protocolo UDP [4].

En enero 11 del 2020, en la revista Electrónica de Estudios Telemáticos, Núñez Stive, en el artículo: "Influencia del volumen de tráfico sobre túnel VPN IPSEC/UDP en enlaces WAN", determina la influencia del volumen de tráfico sobre rendimiento en túnel VPN IPSEC/UDP en enlaces WAN; con el objetivo de establecer una relación entre el volumen de tráfico generado por un constructor de paquetes y el rendimiento de los enlaces con la presencia de redes privadas virtuales utilizando el protocolo IPSEC, en una conexión de tipo puno a punto. Para lo cual, consta de cuatro fases: la primera fase es el diseño, selección del software y hardware. La segunda fase incluye de dos escenarios una al realizar el enlace con túnel y otro sin túnel, de esta forma establece el volumen de tráfico que se necesita para el paquete a transmitir. Tercera

fase: en esta fase, se realiza la captura de los volúmenes de tráfico, registrando los distintos tamaños de archivos transferidos, así como el tiempo requerido en su transmisión. Cuarta fase: se realizan los análisis y cálculos necesarios para generar las curvas y modelado del rendimiento durante la transmisión de datos en el túnel VPN [5].

En Julio 26 del 2020, en la revista tecnología de la informática y las telecomunicaciones, Silvia Monserrate Cedeño Delgado, Dannyll Michellc Zambrano Zambrano, Walter Daniel Zambrano Romero, en el artículo: "Revisión sistemática de Comunicaciones Unificadas de VoIP en redes CAN", menciona que las comunicaciones Unificadas (CU) de VoIP, en la actualidad permiten integrar canales de comunicación tales como correo electrónico, mensajería instantánea, telefonía (fija, móvil, voz sobre IP), videoconferencia, entre otros, funcionando a través de una sola interfaz, permitiendo agilidad y rapidez en los procesos de una organización, mejorando la colaboración e incrementando la productividad de los empleados, habilitando la posibilidad de la movilidad y trabajo remoto, otro aspecto importante en las instituciones es la reducción de costos. Las redes de área de campus (CAN) permiten conectar varias redes LAN a través de un área limitada [6].

En Abril del 2019, en la Revista ResearchGate, Marruecos, Adel Alharbi, Ayoub Bahnasse, en su investigación, "Comparación de la evaluación del rendimiento de VoIP en distintos entornos sobre una red VPN multipunto", menciona que en la última década, VoIP (Voz sobre Protocolo de Internet) es una tecnología en rápido crecimiento que permite transportar voz a través de redes de datos como Internet. Este crecimiento se debe a la integración del sistema VoIP en la infraestructura de red existente y a su bajo coste. Pero consolidar esta infraestructura en toda la red tiene algunos riesgos, ya que las redes de voz están ahora sujetas a virus gusanos, ataques de denegación de servicio (DoS) y otras amenazas bien conocidas. La clave para asegurar la VoIP a través de VPN es utilizar los mecanismos de seguridad como VPN Multipoint. La tecnología VPN Multipoint utiliza mGRE, NHRP, IPSec y protocolos de enrutamiento [7].

En abril 3 del 2019, en la Universidad Peruana de Ciencias Aplicadas, Martel Velasquez, Victor Ronald, en su investigación "Diseño de una red de comunicación

VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764" menciona que las redes de comunicación VPN sobre internet muestra una guía de configuraciones necesarias por requisitos en base al RFC 2764 incluyendo las funcionalidades de la red que permitirá ejecutar las acciones requeridas para agilizar los procesos de negocio mediante un eficiente uso de los recursos TI para la disponibilidad de la información. Además, presenta un diseño de una red de comunicación mediante redes privadas virtuales entre sus locales con el fin de optimizar recursos y agilizar las transacciones diarias propias del giro del negocio, para lo cual el eje principal de la solución es la interconexión de la sede principal y sus sucursales [8].

1.2.1 Contextualización del Problema

En la actualidad, muchas empresas necesitan optimizar sus operaciones e incorporar funciones de red que posibiliten la ejecución ágil de acciones o servicios, lo cual contribuye al crecimiento empresarial en términos de procesos de negocio. Este objetivo se logra mediante el uso de tecnologías de la información que mejoran los servicios ofrecidos, especialmente en lo referente a la disponibilidad de información.

A medida que las empresas buscan expandirse y penetrar en nuevos mercados, surge la necesidad de establecer sucursales adicionales para atender a los clientes. En este sentido, resulta fundamental mantenerse conectado en todo momento y compartir información de manera confiable, rápida y segura. Además, es importante garantizar una accesibilidad económica que permita a las sucursales interactuar en tiempo real para la toma de decisiones y la resolución de problemas.

En el caso específico de las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en Ecuador, se enfrenta el problema de la falta de comunicación en tiempo real entre la sede central y las sucursales, lo cual obstaculiza el crecimiento y la organización de la administración en cada sucursal. Además, no se dispone de un protocolo de seguridad para el flujo de datos en el proceso de comunicación, lo que afecta la disponibilidad de información y conlleva a errores, lentitud y toma de decisiones cautelosa e ineficiente en la Cooperativa.

Por lo tanto, mediante la implementación de una red VPN, la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua, ha obtenido un sistema de comunicación VoIP

privado, lo que permite establecer comunicación directa con las diversas oficinas y departamentos ubicados en distintas ciudades de Ecuador. Asimismo, este sistema facilita video llamadas, así como la realización de conferencias de video a distancia mediante teléfonos IP. Las redes VPN también posibilitan la integración de las cámaras de videovigilancia de todas las sucursales, lo cual permite crear una sala de monitoreo en la oficina central de la Cooperativa.

1.2.2 Fundamentación Teórica

1.2.3 Cooperativa de ahorro y crédito vencedores de Tungurahua.

Un grupo de jóvenes se unieron en el año 2002 para fundar la Cooperativa Vencedores Ltda, cuyo principal propósito es proporcionar servicios de ahorro y crédito a sus usuarios. Su objetivo era brindar el apoyo financiero a los sectores indígenas y campesinos que la banca tradicional no atendía. Después de un proceso organizativo, social y económico, se estableció la COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES DE TUNGURAHUA LTDA en la comunidad de Puganza, parroquia Quisapincha en la Provincia de Tungurahua. El 28 de junio de 2002, el Ministerio de Bienestar Social reconoció la Cooperativa como una sociedad con personería jurídica mediante el Acuerdo No.0020. La Cooperativa inició sus actividades en la misma comunidad de Puganza [9]. En la siguiente figura, se muestra la visión y misión de la Cooperativa.

Figura 1. Misión y visión de la Cooperativa de ahorro y crédito vencedores de Tungurahua [9].

1.2.4 Redes de Comunicación

Una red de comunicaciones se compone de diversos medios técnicos que posibilitan la comunicación a distancia entre equipos autónomos, sin un orden jerárquico (master/slave). Estas redes normalmente se utilizan para transmitir datos, audio y vídeo que generalmente se lo realiza mediante radio enlaces, cable de fibra óptica, cable de cobre entre otros. La información puede ser transmitida en diferentes formatos, como analógico, digital o una combinación de ambos, pero siempre se lleva a cabo las conversiones de forma transparente para el usuario, quien maneja la información de manera analógica exclusivamente. Las redes más comunes son las de ordenadores, las de teléfonos, las de transmisión de audio como sistemas de megafonía o radio ambiental, y las de transmisión de vídeo como la televisión o la videovigilancia y su esquema general se presenta en la figura 2 [10].

Figura 2. Esquema social de una red de comunicación. [11]

1.2.4.1 Parámetros de las redes de comunicación

Los parámetros de las redes de comunicación son medidas utilizadas para describir y evaluar el rendimiento y las características de una red de comunicación. Estos parámetros varían según el tipo de red y los objetivos que se buscan alcanzar. Algunos de los parámetros más importantes que se suelen tener en cuenta en las redes de comunicación son:

Capacidad de transmisión: Es la cantidad de datos que se pueden transmitir por segundo a través de la red. A mayor capacidad de transmisión, mayor cantidad de información se puede transmitir en un tiempo determinado [12].

Velocidad de transmisión: Es el tiempo que tarda la información en transmitirse desde un punto a otro de la red. A mayor velocidad de transmisión, menor es el tiempo que se tarda en enviar la información [12].

Latencia: Es el tiempo que tarda un paquete de datos en llegar desde el origen hasta el destino. Una latencia alta puede generar problemas en la comunicación en tiempo real, como en el caso de las videoconferencias [12].

Fiabilidad: Es la capacidad de la red para transmitir los datos de forma correcta y sin errores. Una red poco fiable puede provocar la pérdida o corrupción de datos importantes [12].

Seguridad: Es la capacidad de la red para proteger los datos y la información transmitida de accesos no autorizados o ataques cibernéticos [12].

Cobertura: Es la capacidad de la red para cubrir una determinada área geográfica. A mayor cobertura, mayor será el área que se puede cubrir con la red [12].

1.2.4.2 Topologías de Red

Las topologías de red son una forma de representar la estructura y organización de los nodos o dispositivos en una red de computadoras. Esto incluye la forma en que los dispositivos están interconectados, cómo se transmiten los datos entre ellos y cómo se gestiona el flujo de información en la red. En general, la topología de una red se refiere a la forma física y lógica en que se conectan los nodos de la red. La topología puede ser determinante para la eficiencia, velocidad y seguridad de la red, y es un factor importante para considerar al diseñar o implementar una red de computadoras [13]. Entre las principales topologías se tiene:

Topología en bus

La topología en Bus se refiere a un tipo de estructura de red en la que todos los dispositivos o nodos de la red se conectan a un único medio de transmisión conocido

como "bus". En esta topología, los nodos intercambian datos a través del mismo cable, lo que significa que si el cable falla, la red completa puede sufrir una interrupción. Cada nodo en una topología de Bus se conecta al bus de la red a través de un conector BNC. El cable se extiende desde un extremo de la red hasta el otro, conectando todos los nodos en serie. Todos los nodos reciben los datos transmitidos a través del bus, pero solo el destinatario procesa y responde a los datos como se observa en la figura 3[14].

Aunque la topología en Bus es una de las topologías más simples y antiguas, todavía se usa en algunas redes pequeñas debido a su bajo costo y facilidad de instalación. Sin embargo, su uso ha disminuido debido a la posibilidad de una falla del cable que podría afectar a toda la red y a la necesidad de coordinación en el acceso al bus por parte de los nodos, lo que puede reducir la eficiencia de la red [14].

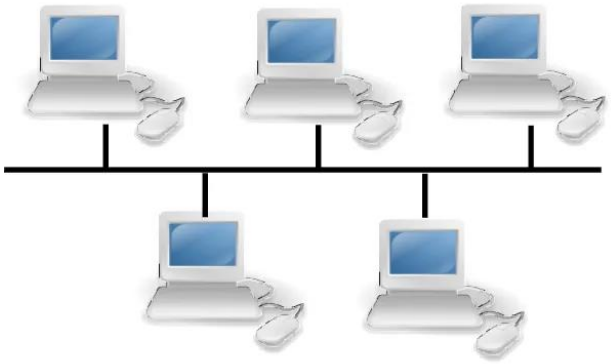


Figura 3. Esquema de red de una topología en bus [14].

Ventajas y desventajas

La topología de red en bus, tiene ventajas y desventajas que deben ser consideradas cuidadosamente antes de su implementación. En la tabla 1, se presentan algunos aspectos importantes a tener en cuenta para evaluar su uso.

Tabla 1. Ventajas y desventajas de la topología en bus

Ventajas y desventajas de la topología de red en bus	
Ventajas	**Desventajas**
Facilidad de instalación	Menos confiable que otras topologías de red
Bajo costo de implementación	Si se agregan demasiados nodos a la red, la velocidad de transmisión de los datos puede disminuir significativamente.
Fácil de mantener, ya que se pueden agregar o eliminar nodos sin interrumpir el funcionamiento de la red	Mayor posibilidad de colisiones de datos, ya que todos los nodos compiten por el mismo medio de transmisión
Cada nodo en la red puede recibir y enviar datos a través del mismo cable, lo que la hace adecuada para redes pequeñas y de baja complejidad.	No proporciona privacidad o seguridad para los datos transmitidos, cualquier nodo en la red puede interceptar los datos que se envían a través del cable
Las fallas en infraestructura son mínimas	La necesidad de coordinar el acceso al bus por parte de los nodos puede reducir la eficiencia de la red

Elaborado por: El investigador basado en [14].

Topología en estrella

La topología en estrella es un tipo de estructura de red en el que todos los nodos de la red están conectados a un dispositivo central, como un hub o switch, mediante un cable de conexión dedicado. Esto significa que todos los nodos se comunican a través del dispositivo central en lugar de conectarse directamente entre sí. El hub o switch actúa como un punto central de control que administra el tráfico de la red y puede retransmitir los datos a su destino correspondiente [15].

Cada nodo en la red tiene su propia conexión dedicada al dispositivo central como se observa en la figura 4, lo que significa que, si falla un nodo, no afecta el

funcionamiento de los demás nodos en la red. Además, la topología en estrella es fácil de instalar y configurar, lo que la convierte en una opción popular para redes de tamaño mediano a grande. Al centralizar el tráfico de la red, el dispositivo central facilita la identificación de problemas de conectividad. A pesar de que el hub o switch puede ser un punto único de falla, la topología en estrella sigue siendo una opción popular debido a su alta escalabilidad y facilidad de uso en la administración de redes empresariales y de oficina [15].

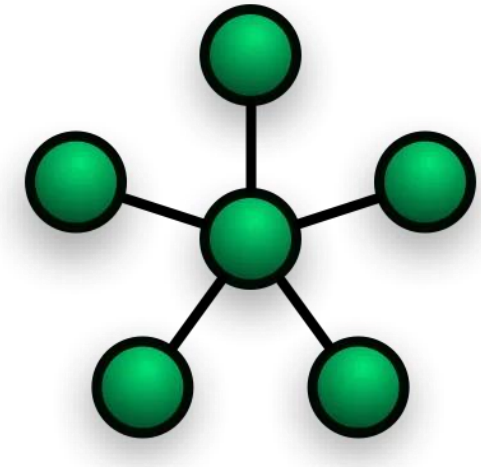


Figura 4. Topología en estrella [14].

Ventajas y desventajas

La topología de red en estrella tiene ventajas y desventajas a la hora de su implementación como se muestra en la tabla 2 en donde se presentan algunos aspectos importantes a tener en cuenta para evaluar su uso.

Tabla 2. Ventajas y desventajas de la topología en estrella.

Ventajas y desventajas de la topología de red en estrella	
Ventajas	**Desventajas**
La resolución de problemas en la topología en estrella es más eficiente en comparación con topologías anteriores	El hub o switch central es un punto único de fallo. Si falla, toda la red podría verse afectada.

Permite un control centralizado de la red, lo que permite una gestión directa con cada cliente	Requiere más cables que otras topologías, lo que puede aumentar los costos de instalación y mantenimiento de la red
Si un cable de un cliente falla, no afectará a la red y su detección y corrección es más rápida en la topología en estrella	Cada nodo se conecta directamente al hub o switch, existe una limitación en la distancia que puede haber entre el dispositivo central y cada nodo
Utiliza herramientas económicas y disponibles para su mantenimiento e instalación	Existe una capacidad limitada en cuanto al número de nodos que se pueden conectar a la red antes de que se vea afectada la velocidad y el rendimiento de la red

Elaborado por: El investigador basado en [15].

Topología en anillo

La topología de anillo es una estructura de red en la que los dispositivos están conectados en una ruta circular formando una conexión continua para la transmisión de señales como se muestra en la figura 5. También llamada red de anillo o topología activa, esta configuración es altamente eficiente y maneja mejor el tráfico pesado que la topología de bus. Cada dispositivo está conectado a otros dos, uno delante y otro detrás, y los mensajes van pasando por cada dispositivo en el anillo. La mayoría de las configuraciones de anillo permiten que los datos se desplacen en un solo sentido, denominada unidireccional, aunque algunas también permiten que los paquetes viajen en ambos sentidos, conocida como bidireccional. La topología de anillo es ideal para redes en las que se necesita un alto rendimiento y no se toleran interrupciones, ya que, en caso de fallo de un dispositivo, la señal puede seguir fluyendo en la dirección opuesta [16].

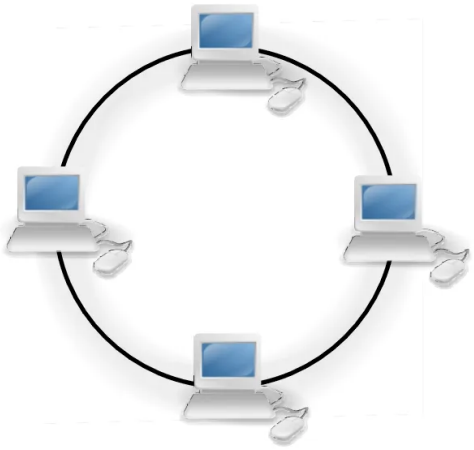


Figura 5. Topología en anillo [14]

Ventajas y Desventajas

En la implementación de la topología de red en anillo es necesario considerar tanto sus ventajas como sus desventajas. La tabla 3, muestra algunos aspectos importantes que deben ser evaluados para determinar la idoneidad de esta topología en una red específica.

Tabla 3. Ventajas y desventajas de la topología en anillo.

Ventajas y desventajas de la topología de red en anillo	
Ventajas	**Desventajas**
No es necesario un servidor de red o un concentrador central para administrar la conectividad entre cada estación de trabajo en la red.	Un solo corte en el cable de la red puede interrumpir toda la comunicación en la red.
La instalación y resolución de problemas en este tipo de red es relativamente sencilla	Dificultad para agregar o eliminar nodos: La adición o eliminación de nodos en la red puede ser complicada y puede afectar la actividad de la red.
La transferencia de datos entre estaciones de trabajo puede ocurrir a velocidades elevadas.	Todos los datos que se transmiten a lo largo de la red deben pasar por cada estación de trabajo en la red, lo que puede disminuir la velocidad de la transferencia

	de datos en comparación con la topología en estrella.
La red de anillo puede manejar un gran volumen de nodos en una sola red	El hardware necesario para conectar cada estación de trabajo a la red es más costoso que las tarjetas Ethernet y concentradores o conmutadores de la topología en estrella.
Es más fácil solucionar los problemas en esta topología debido a que las fallas en los cables pueden ser detectadas y localizadas sin complicaciones.	En las redes unidireccionales, los paquetes de datos deben pasar por todos los dispositivos de la red para llegar a su destino, lo que puede aumentar el tiempo de transmisión y reducir la eficiencia de la red.

Elaborado por: El investigador basado en [16].

Topología en malla

Una red de malla se caracteriza por la interconexión de dispositivos o nodos entre sí como se muestra en la figura 6, lo que permite una eficaz transmisión de datos entre ellos y con los clientes. Esta topología de red es altamente resistente ante fallos de un nodo o conexión, ya que se crean múltiples rutas para el tráfico de datos. Además, las redes de malla pueden contar con una gran cantidad de nodos inalámbricos y otros dispositivos como routers y conmutadores. Es importante destacar que existen dos tipos de topologías de red de malla: completa y parcial. En la topología de malla completa, cada nodo está conectado directamente a todos los demás, mientras que en la topología de malla parcial, solo algunos nodos se conectan directamente entre sí, lo que puede generar la necesidad de que los nodos pasen por otros para llegar a su destino final [17].

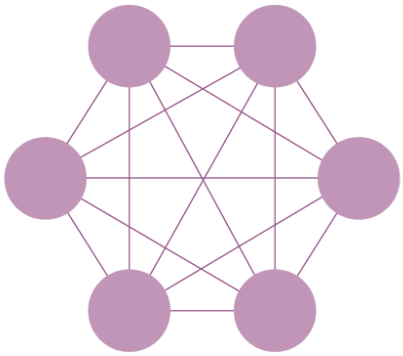


Figura 6. Topología en malla [17].

Ventajas y Desventajas

Es importante evaluar tanto las ventajas como las desventajas antes de implementar la topología de red en malla. La tabla 4, presenta algunos aspectos importantes a tener en cuenta para evaluar la idoneidad de esta topología en una red específica.

Tabla 4. Ventajas y desventajas de la topología en malla.

Ventajas y desventajas de la topología de red en malla	
Ventajas	**Desventajas**
Mayor estabilidad debido a que un fallo en un punto no afecta a toda la red	Los nodos individuales tienen un alcance más limitado
Mayor alcance y menos puntos muertos para la señal Wi-Fi	La ampliación de la red puede ser un desafío debido a la cantidad de nodos necesarios
Los nodos pueden comunicarse directamente entre sí, sin la necesidad de un punto de acceso central	Cuanto más compleja sea la red de malla, más difícil será su gestión y solución de problemas
Mayor seguridad, ya que los nodos individuales pueden ser fácilmente reemplazados en caso de un ataque	Puede haber problemas de latencia con redes de baja potencia, ya que la capacidad de procesamiento puede ser insuficiente para gestionar la mensajería

Elaborado por: El investigador basado en [17].

Topología en árbol

La topología en árbol es una estructura de red que se organiza de manera jerárquica, donde los nodos se conectan en forma de árbol. A diferencia de la topología de estrella, que tiene un nodo central, la topología en árbol se compone de un punto raíz del que se despliegan ramificaciones hacia otros nodos, creando una estructura escalonada. La topología en árbol puede ser vista como una combinación de múltiples redes en estrella interconectadas entre sí como se observa en la figura 7. Además, la conexión en árbol tiene similitudes con la topología en bus cuando el nodo de interconexión trabaja en modo de difusión, ya que la información se propaga hacia todas las estaciones. Sin embargo, en la topología en árbol, las ramificaciones se extienden desde un punto raíz a tantas ramas como sean necesarias, según las necesidades de la red. En general, la topología en árbol es una estructura de red escalable y jerarquizada que se utiliza en muchas organizaciones debido a su capacidad para soportar grandes cantidades de tráfico y permitir una fácil expansión de la red [18].

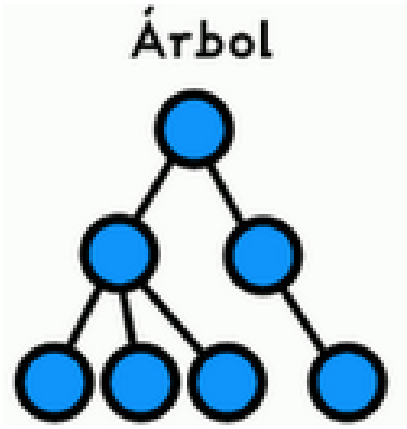


Figura 7. Topología en árbol [18].

Ventajas y Desventajas

Antes de implementar la topología de red en árbol, es fundamental llevar a cabo una evaluación exhaustiva de sus ventajas y desventajas. Para tal fin, es de gran utilidad considerar los aspectos relevantes que se presentan en la tabla 6, ya que permiten determinar la viabilidad y conveniencia de utilizar esta topología en una red particular. Es importante realizar un análisis detallado para poder tomar decisiones informadas y asegurar una implementación exitosa de la red en malla.

Tabla 5. Ventajas y desventajas de la topología en árbol.

Ventajas y desventajas de la topología de red en árbol	
Ventajas	**Desventajas**
La señal se amplifica y su alcance se extiende al pasar a través del Hub central, lo que aumenta su potencia y distancia	En caso de que el cableado principal presente algún problema, toda la red puede verse afectada ya que depende de él para su funcionamiento.
Se pueden conectar más dispositivos a través de la inclusión de concentradores secundarios	Si la ruta de conexión de un nodo individual falla, este puede quedar desconectado de la red
Es posible dar prioridad y aislar las comunicaciones de distintos equipos, y también es posible implementar un cableado punto a punto para segmentos individuales.	Se requiere la inclusión de concentradores para asegurar que los distintos grupos o ramificaciones del árbol mantengan una conexión estable con el resto de la red.
La tecnología de Hub es compatible con muchos proveedores de hardware y software.	Debido al tamaño de la red en árbol, su mantenimiento puede resultar complicado y costoso.

Elaborado por: El investigador basado en [18].

1.2.4.3 Tipos de Red

Los tipos de red se refieren a las diversas formas en que se pueden organizar los dispositivos de comunicación en una red de computadoras. Es decir, se trata de una clasificación de las redes según su configuración y la topología de conexión de los dispositivos. Existen varios tipos de redes, y cada una tiene sus propias ventajas e inconvenientes, dependiendo del uso previsto y de las necesidades de los usuarios. Entre los tipos de red más comunes, se encuentran:

Red de área local (LAN): es una red de computadoras que se encuentra en un área geográfica limitada, como una oficina, un edificio o una escuela. Estas redes suelen ser de alta velocidad y pueden ser cableadas o inalámbricas [19].

Red de área amplia (WAN): es una red que abarca una gran área geográfica, como una ciudad, un país o incluso varios países. Las WAN suelen utilizar tecnologías de comunicación de larga distancia, como líneas telefónicas, satélites o fibra óptica [19].

Red de área personal (PAN): son una red de computadoras interconectadas que se utiliza para la comunicación entre dispositivos cercanos a una persona, generalmente dentro de un radio de unos pocos metros [19].

Red de área de almacenamiento (SAN): es una red que se utiliza para conectar dispositivos de almacenamiento, como discos duros, a los servidores y a otros dispositivos de almacenamiento. Las redes SAN suelen ser muy rápidas y están diseñadas para manejar grandes cantidades de datos [19].

Red de área metropolitana (MAN): es una red que se extiende sobre una ciudad o una zona metropolitana. Las MAN suelen utilizarse para conectar varias LAN en una sola red [19].

Red de campus: es una red que abarca un campus universitario o un complejo de edificios. Estas redes suelen ser grandes y están diseñadas para manejar grandes cantidades de tráfico [19].

Red de internet: es una red global que conecta a millones de computadoras y dispositivos en todo el mundo. La Internet es la red más grande del mundo y se utiliza para transmitir todo tipo de información, desde correos electrónicos hasta videos y juegos en línea [19].

La figura 8, muestra un diagrama que ilustra las características de los tipos de red más importantes.

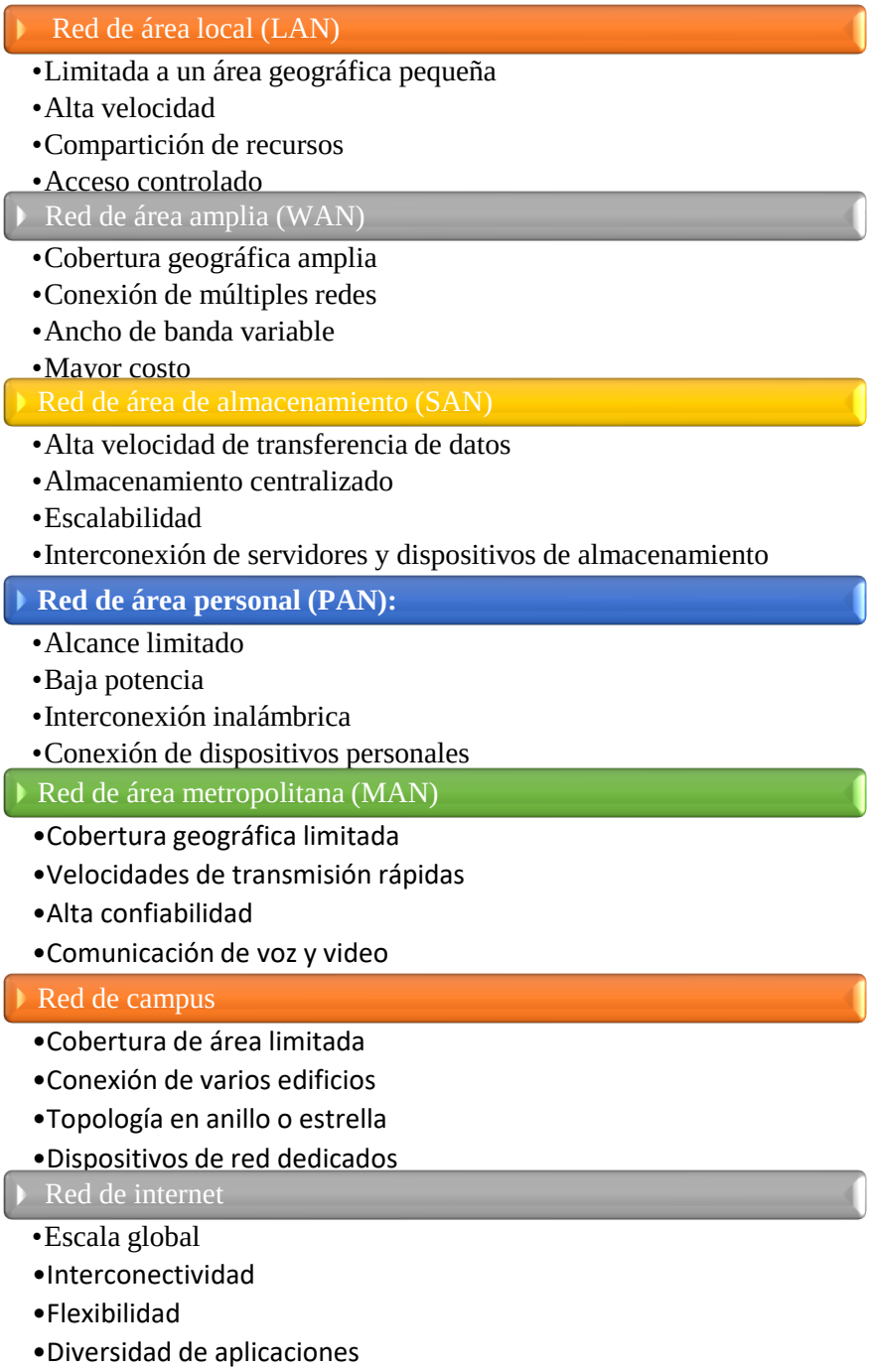


Figura 8. Diagrama de las características de los tipos de redes.

Elaborado por: El investigador basado en [19].

1.2.4.4 Servicios de Red

Los servicios de red proporcionan funciones específicas a los usuarios y dispositivos conectados a la red. Estos servicios pueden incluir, entre otros, el acceso a internet, la

impresión en red, el intercambio de archivos, el correo electrónico, la mensajería instantánea, la videoconferencia, la gestión de bases de datos, la seguridad de la red y la administración remota de dispositivos. Los servicios de red son fundamentales para permitir una comunicación y colaboración efectiva en la red, y para garantizar que la red funcione de manera segura, eficiente y confiable [20]. En el diagrama de la figura 9, se establece los principales servicios de red que se pueden implementar.

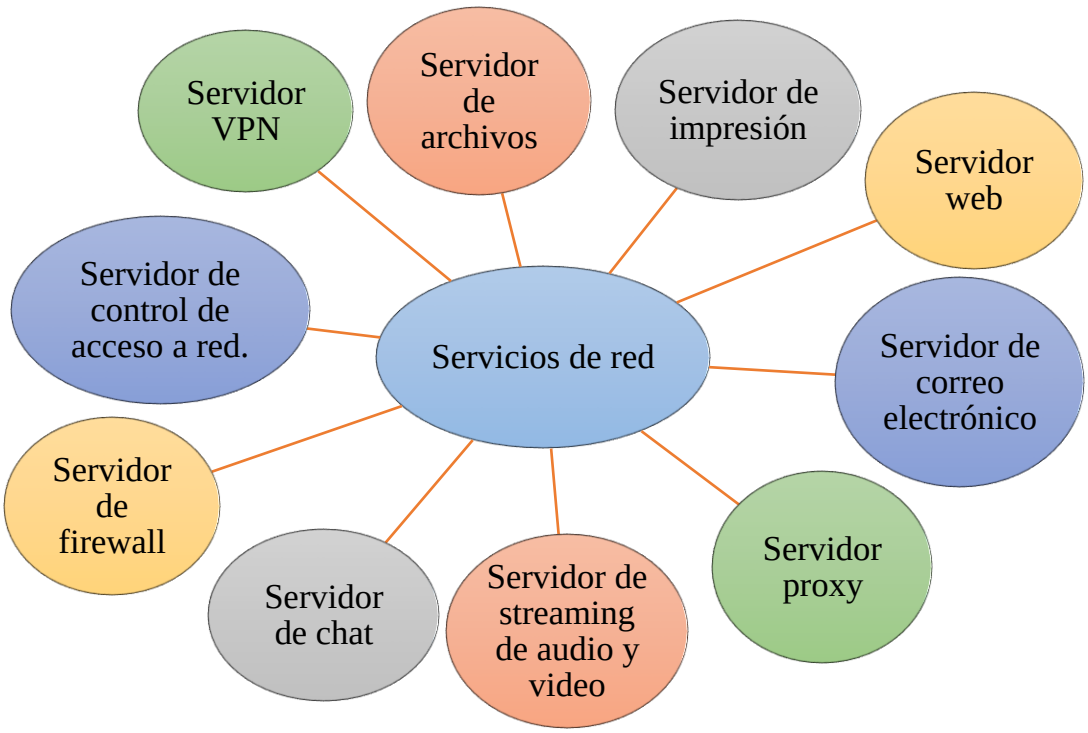


Figura 9. Servicio de Red

Elaborado por: El investigador basado en [21]

1.2.4.5 Protocolos de Red

Los protocolos de red son un conjunto de reglas y estándares que permiten la comunicación y el intercambio de datos entre dispositivos en una red de computadoras. Los protocolos establecen cómo los datos deben ser formateados, transmitidos, recibidos y procesados, asegurando así que la comunicación sea confiable, eficiente y segura.

Existen muchos protocolos de red, cada uno diseñado para un propósito específico. Por ejemplo, algunos protocolos están diseñados para la transmisión de datos en

tiempo real, como el protocolo de voz sobre IP (VoIP), mientras que otros están diseñados para la transferencia de archivos, como el protocolo de transferencia de archivos (FTP). También existen protocolos de red para la gestión de red, como el protocolo simple de administración de red (SNMP), que permite a los administradores de red monitorear y controlar los dispositivos de red desde un lugar centralizado [22]. Entre los principales protocolos se tiene:

Protocolo de configuración dinámica de host (DHCP)

El protocolo mencionado es un estándar del grupo de Trabajo de Ingeniería de Internet, cuyo propósito es reducir la carga administrativa y la complejidad de la configuración de los hosts en los protocolos de control de transmisión basados en la red. El proceso de configuración de este protocolo se realiza automáticamente cuando el equipo utiliza clientes para solicitar y aceptar información de configuración TCP/IP de los servidores DHCP. La gestión de direcciones IP y otros parámetros relacionados con la configuración también es manejada por este protocolo, el cual utiliza agentes de transmisión DHCP para transferir información entre el servidor y el cliente de manera constante [21].

Protocolo simple de Administración de red (SNMP)

El protocolo mencionado se utiliza principalmente para administrar redes TCP/IP y es una de las más utilizados debido a su fácil implementación y bajo consumo de recursos y red. La versión más avanzada, SNMPv2, es compatible con redes basadas en OSI. Este protocolo funciona a través del envío de mensajes a diferentes ubicaciones de la red mediante Protocolos de Unidad de Datos (PUD), y consta de dos elementos: los agentes y las estaciones de trabajo. Los agentes son elementos incorporados en dispositivos de red como servidores, routers y switches, y son responsables de recopilar y almacenar información a nivel local para su acceso posterior. Cada agente tiene una base de información de gestión local relevante [21].

Domain Name System (DNS)

El DNS, que significa Sistema de Nombres de Dominio en inglés, es un servicio fundamental para la navegación en Internet. En pocas palabras, se trata de una especie de guía telefónica virtual que asocia los nombres de dominio de los sitios web con sus

respectivas direcciones IP. De esta forma, cuando un usuario ingresa una dirección web en su navegador, el DNS es el encargado de buscar la dirección IP correspondiente y redirigir la petición a ese servidor. Este proceso de conversión de nombres de dominio en direcciones IP es esencial para la navegación en Internet, ya que resultaría muy complicado recordar una serie de números para acceder a cada sitio web. Además, el DNS no solo es útil para los usuarios, sino también para los propietarios de sitios web, ya que les permite cambiar la dirección IP de sus servidores sin tener que modificar todos los enlaces y referencias a su sitio en Internet.

Por otro lado, es importante mencionar que existen diferentes tipos de servidores DNS, entre ellos los servidores raíz, los servidores de nivel superior y los servidores de nivel inferior. Cada uno de ellos cumple una función específica en la resolución de nombres de dominio y en la distribución de la información entre los diferentes servidores DNS que existen en el mundo [21].

Transferencia de archivos (FTP)

El objetivo de este protocolo es permitir que los usuarios puedan intercambiar información de manera sencilla y rápida entre distintos ordenadores a través de Internet. Para esto, se utiliza TCP/IP y el protocolo de control de transmisión, que se encargan de gestionar la carga y descarga de archivos. En el caso específico del FTP, es necesario que tanto el servidor como el cliente tengan sus puertos abiertos para que se pueda llevar a cabo el intercambio de información. De esta manera, cuando se utiliza FTP, el ordenador establece una comunicación con el puerto adyacente para recibir información del controlador y determinar la dirección IP a la que se desea transferir el archivo [21].

1.2.4.6 Enrutamiento

El enrutamiento de redes es un procedimiento fundamental para elegir el camino más eficiente a través de una o varias redes. Este proceso es aplicable a diversos tipos de redes, que van desde las redes telefónicas hasta el transporte público. En las redes de conmutación de paquetes, como lo es el caso de Internet, el enrutamiento es crucial para seleccionar las rutas adecuadas para que los paquetes de Protocolo de Internet (IP) como se visualiza en la figura 11, puedan llegar sin problemas desde su origen hasta su destino final. Este proceso de enrutamiento en Internet es llevado a cabo por

dispositivos especializados de hardware de red, también conocidos como enrutadores, que se encargan de tomar las decisiones adecuadas para que los paquetes lleguen a su destino de manera eficiente [23].

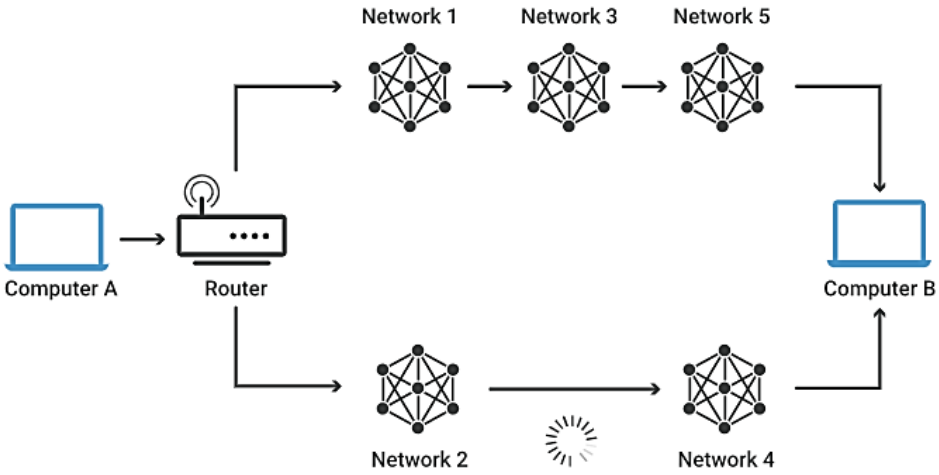


Figura 10. Esquema lógico del enrutamiento [23].

Funcionamiento del enrutamiento

Los enrutadores utilizan tablas de enrutamiento internas para tomar decisiones sobre cómo dirigir los paquetes a través de las rutas de red. Estas tablas registran las rutas necesarias para que los paquetes lleguen a su destino, y funcionan de manera similar a los horarios de tren que los pasajeros consultan para elegir el tren adecuado. Al recibir un paquete, el enrutador lee la información de destino del encabezado del paquete, al igual que un revisor de tren comprueba los billetes para determinar en qué tren debe ir un pasajero, y luego determina la ruta adecuada basándose en la información de sus tablas de enrutamiento [23].

Este proceso se realiza en tiempo real y a gran velocidad, ya que los enrutadores pueden procesar millones de paquetes por segundo y dirigirlos a través de varios enrutadores hasta que lleguen a su destino. Las tablas de enrutamiento pueden ser estáticas o dinámicas. Las tablas de enrutamiento estáticas se configuran manualmente por un administrador de red y establecen las rutas que los paquetes de datos deben seguir a través de la red, a menos que el administrador actualice las tablas manualmente [23].

Tipos de enrutamiento

Existen varios tipos de enrutamiento en redes, los cuales se utilizan para diferentes propósitos y situaciones. A continuación, se describen dos enrutamientos conocidos como estático y dinámico:

Enrutamiento Estático

El enrutamiento estático es un método en el que el administrador de red establece manualmente las rutas para que los paquetes de datos viajen a través de la red. Esto significa que las rutas utilizadas por los paquetes son predefinidas y no cambian automáticamente si las condiciones de la red se modifican. El administrador de red configura las rutas a través de una tabla de enrutamiento estática, lo que permite que los enrutadores envíen el tráfico a través de una ruta específica. Sin embargo, si se desea modificar las rutas, la tabla de enrutamiento debe ser actualizada manualmente [24].

Este tipo de enrutamiento es comúnmente utilizado en redes pequeñas y sencillas, donde la topología de la red no sufre cambios con frecuencia. A diferencia del enrutamiento dinámico, no requiere un protocolo de enrutamiento para actualizar la tabla de enrutamiento, lo que puede facilitar la administración y configuración de la red. No obstante, una desventaja es que no se adapta bien a cambios en la red, y puede requerir mucho tiempo y esfuerzo para actualizar manualmente las tablas de enrutamiento en caso de cambios en la topología de la red [24]. En la tabla 6 se presenta las características principales del enrutamiento estático.

Enrutamiento Dinámico

El enrutamiento dinámico se refiere a un proceso de enrutamiento donde los enrutadores en la red intercambian información automáticamente y ajustan sus rutas en función de las condiciones de la red. En lugar de que un administrador configure manualmente las rutas, los protocolos de enrutamiento dinámico, como OSPF o RIP, permiten que los enrutadores aprendan las rutas y actualicen sus tablas de enrutamiento automáticamente [24].

En el enrutamiento dinámico, los enrutadores intercambian información sobre las rutas de la red utilizando algoritmos. Cada enrutador tiene una tabla de enrutamiento

dinámica que se actualiza automáticamente en función de la información intercambiada con los enrutadores vecinos. Además, estos protocolos pueden ajustar las rutas automáticamente en caso de fallos en la red o cambios en la topología [24].

El enrutamiento dinámico se utiliza generalmente en redes grandes y complejas, ya que permite una administración más eficiente y adaptativa de la red. Los protocolos de enrutamiento dinámico también pueden ser configurados para evitar bucles de enrutamiento y mejorar la eficiencia de la red. Aunque pueden requerir una mayor configuración y monitoreo para garantizar el funcionamiento correcto y estable de la red [24].

En la tabla 6, se presentan las características y diferencias entre el enrutamiento estático y dinámico.

Tabla 6. Características y diferencias de los tipos de enrutamiento [24].

Característica	**Routing estático**	**Routing dinámico**
Complejidad de la configuración	Incrementos en la magnitud referente a la red	Independiente del tamaño que se tenga de la red
Cambios de topología	Para cambios en la topología se requiere la intervención de un administrador de redes	Se adapta a los cambios de topología automáticamente
Escalabilidad	Se utiliza mayormente en topologías simples	Es más utilizado en topologías más complejas
Seguridad	La seguridad es en este enrutamiento es inherente	La seguridad en este enrutamiento debe estar configurada
Uso de recursos	No es necesario utilizar recursos adicionales	Usa CPU, memoria, ancho de banda de enlaces
Predictibilidad de Ruta	La predictibilidad de ruta está definida explícitamente por el administrador	La ruta que se utiliza para enrutar el tráfico en una red depende tanto de la topología de la red como del protocolo de enrutamiento que se esté utilizando

Elaborado por: El investigador basado en [24].

Tanto el enrutamiento dinámico como el estático son métodos válidos para establecer rutas de red en un entorno informático. Cada método tiene sus propias ventajas y desventajas, y la elección entre uno y otro dependerá de las necesidades y requisitos

específicos de cada red. El enrutamiento estático ofrece un mayor control y predictibilidad en la configuración de rutas, mientras que el enrutamiento dinámico se adapta automáticamente a los cambios en la topología de la red. Es importante evaluar cuidadosamente las necesidades de la red y considerar los factores de seguridad, rendimiento y escalabilidad al decidir qué método de enrutamiento utilizar.

1.2.5 Túneles VPN

Un túnel VPN es una conexión segura que se establece entre dos redes diferentes a través de una red pública, como Internet. Esta conexión se utiliza para proteger la privacidad y seguridad de las comunicaciones entre las redes, lo que resulta especialmente importante en el intercambio de información confidencial y en la conexión de redes corporativas desde ubicaciones remotas. Durante el proceso de conexión de un túnel VPN, se crea un canal cifrado entre los puntos finales de la conexión. Este canal se utiliza para transportar los datos entre las redes, y los paquetes de datos se encapsulan en paquetes adicionales para asegurar su integridad y confidencialidad como se observa en la figura 12. El cifrado de los datos y la encapsulación en paquetes adicionales hacen que sea más difícil para los hackers interceptar y leer los datos transmitidos entre las redes [25].

Los túneles VPN se utilizan comúnmente en el entorno empresarial para conectar redes corporativas a través de Internet, permitiendo que los empleados accedan a los recursos de la red de la empresa desde ubicaciones remotas de forma segura. Además, se pueden utilizar para conectarse a servicios en línea restringidos geográficamente, como servicios de streaming, que sólo están disponibles en ciertas regiones. En definitiva, los túneles VPN ofrecen una forma segura y eficaz de conectar redes separadas y garantizar la privacidad y seguridad de las comunicaciones [25].

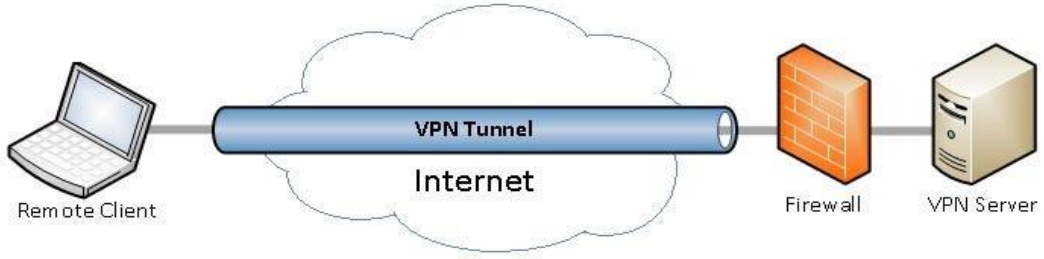


Figura 11. Conexión estándar de un túnel VPN [26].

1.2.5.1 Ventajas y desventajas de los túneles VPN

La implementación de túneles VPN puede ofrecer varias ventajas para su uso en diferentes aspectos o parámetros de implementación, sin embargo, también es importante considerar ciertas desventajas que puedan surgir.

Ventajas

- Seguridad: El uso de un túnel VPN proporciona una conexión segura entre dos redes separadas. Los datos que se transmiten a través del túnel están protegidos mediante cifrado, lo que significa que sólo las partes autorizadas pueden acceder a ellos.
- Accesibilidad remota: Los túneles VPN permiten a los usuarios acceder a la red de la empresa desde ubicaciones remotas. Esto es especialmente útil para los trabajadores que necesitan acceder a recursos de la empresa mientras están fuera de la oficina.
- Costo-efectividad: En comparación con la implementación de una conexión dedicada, los túneles VPN pueden ser más rentables. Esto se debe a que los túneles VPN utilizan infraestructuras de red existentes, como Internet, en lugar de requerir la instalación de líneas dedicadas [27].

Desventajas

- Rendimiento: El uso de un túnel VPN puede afectar el rendimiento de la conexión a Internet. La sobrecarga adicional del cifrado y la encapsulación de los datos pueden disminuir la velocidad y aumentar la latencia.
- Configuración y mantenimiento: La configuración y el mantenimiento de los túneles VPN pueden ser complejos y requerir conocimientos técnicos especializados. Además, las actualizaciones de software y los cambios en la red pueden requerir ajustes en la configuración de los túneles VPN.
- Seguridad: Aunque los túneles VPN son una forma segura de proteger las comunicaciones en línea, no son infalibles. Es posible que se produzcan fallos de seguridad, como fugas de datos, que comprometan la seguridad de la conexión VPN [27].

1.2.5.2 Protocolos de interconexión de túneles VPN

Los protocolos de túneles VPN son tecnologías y estándares que permiten establecer una conexión segura y privada entre dos dispositivos a través de Internet. Para lograr esto, los datos que se transmiten entre los dispositivos son encapsulados dentro de paquetes protegidos por un protocolo de cifrado, lo que los hace inaccesibles a otros dispositivos o personas en la red pública. Los protocolos de túneles VPN establecen la forma en que se gestiona y se establece el túnel, así como la forma en que se autentican los usuarios y dispositivos. También definen cómo se cifran y descifran los datos y cómo se garantiza la integridad de estos durante su transmisión [28].

Existen varios protocolos de túneles VPN disponibles, cada uno con diferentes características y niveles de seguridad. La elección del protocolo dependerá de las necesidades específicas del usuario o empresa, así como de la compatibilidad y facilidad de uso en los dispositivos y sistemas operativos que se utilicen [28].

Protocolo de túnel punto a punto (PPTP)

Es un protocolo de túnel VPN (Red Privada Virtual) que se utiliza para establecer conexiones seguras entre dispositivos a través de Internet. PPTP fue desarrollado en la década de 1990 como una solución fácil de implementar y compatible con una amplia variedad de sistemas operativos. Funciona encapsulando los datos que se transmiten entre los dispositivos en paquetes protegidos por un protocolo de cifrado [28].

Sin embargo, PPTP se ha vuelto menos popular debido a sus limitaciones de seguridad. El cifrado utilizado por PPTP es débil y puede ser fácilmente violado. Además, PPTP no es compatible con IPv6 y puede tener problemas de compatibilidad con algunos dispositivos de red, como firewalls y routers [28].

Protocolo de túnel de capa 2 (L2TP)

PPTP (Protocolo de túnel punto a punto) es un protocolo de túnel VPN (Red Privada Virtual) que se utiliza para establecer conexiones seguras entre dispositivos a través de Internet. PPTP fue desarrollado en la década de 1990 como una solución fácil de implementar y compatible con una amplia variedad de sistemas operativos. Funciona encapsulando los datos que se transmiten entre los dispositivos en paquetes protegidos

por un protocolo de cifrado. Sin embargo, PPTP se ha vuelto menos popular debido a sus limitaciones de seguridad. El cifrado utilizado por PPTP es débil y puede ser fácilmente violado. Además, PPTP no es compatible con IPv6 y puede tener problemas de compatibilidad con algunos dispositivos de red, como firewalls y routers [28].

Características

- Facilidad de implementación: PPTP fue diseñado para ser fácil de implementar en diferentes sistemas operativos, lo que lo hace popular en entornos de red heterogéneos.
- Compatibilidad: PPTP es compatible con una amplia variedad de dispositivos de red, como routers, firewalls y servidores VPN.
- Velocidad: PPTP es uno de los protocolos VPN más rápidos debido a su bajo costo computacional, lo que lo hace adecuado para aplicaciones que requieren una conexión VPN rápida.
- Soporte integrado: PPTP se incluye en muchos sistemas operativos, lo que significa que no es necesario instalar software adicional para utilizarlo.
- Limitaciones de seguridad: PPTP utiliza un cifrado débil que se considera vulnerable a los ataques de fuerza bruta, lo que lo hace inadecuado para aplicaciones que requieren una alta seguridad.
- Falta de soporte IPv6: PPTP no es compatible con el protocolo IPv6, lo que significa que no puede utilizarse en redes que utilicen este protocolo.

Protocolo de seguridad de Internet (IPSec)

El Protocolo de seguridad de Internet (IPSec) es una tecnología de seguridad que se utiliza en las redes de computadoras para asegurar las conexiones entre dispositivos. El funcionamiento de IPSec se basa en la creación de un túnel VPN entre dos dispositivos, lo que permite que los datos se transmitan de manera segura y privada a través de Internet. Para garantizar la seguridad de los datos, IPSec utiliza técnicas de cifrado y autenticación de paquetes de datos que se envían entre los dispositivos [28].

IPSec es ampliamente utilizado en la industria de redes debido a su compatibilidad con una amplia variedad de dispositivos de red y sistemas operativos. También es compatible con las versiones de protocolo de Internet IPv4 e IPv6, y puede ser

utilizado para asegurar el tráfico de red en entornos públicos y privados. Además, IPSec permite establecer conexiones VPN de sitio a sitio, lo que permite la conexión segura y privada de dos redes diferentes [28].

Características

- Seguridad: IPSec proporciona un alto nivel de seguridad al cifrar los datos transmitidos entre dos dispositivos y autenticar la identidad de los dispositivos para evitar la suplantación de identidad.
- Flexibilidad: IPSec es compatible con una amplia variedad de dispositivos de red y sistemas operativos, lo que lo hace adecuado para su uso en una amplia gama de entornos de red.
- Escalabilidad: IPSec se puede utilizar para asegurar tanto redes grandes como pequeñas, y se puede adaptar a diferentes requisitos de red.
- Conexiones VPN: IPSec se utiliza comúnmente para establecer conexiones VPN, lo que permite la conexión segura de dispositivos remotos y la creación de redes privadas virtuales.
- Compatibilidad con IPv4 e IPv6: IPSec es compatible con ambos protocolos de Internet, lo que lo hace adecuado para su uso en entornos de red actuales y futuros.
- Gestión de políticas: IPSec proporciona herramientas para la gestión de políticas de seguridad y permite a los administradores de red definir reglas de seguridad específicas para los dispositivos y usuarios de la red.
- Protección de integridad: IPSec garantiza la integridad de los datos transmitidos a través de la red, asegurando que los datos no sean manipulados o alterados durante la transmisión [28].

Capa de sockets seguros (SSL)

La Capa de sockets seguros (SSL) es un protocolo de seguridad que establece una conexión cifrada y segura entre dos dispositivos en una red de computadoras. Fue desarrollado por Netscape en la década de 1990 y se utiliza ampliamente para proteger la transmisión de datos en línea, incluyendo transacciones financieras y el acceso a sitios web seguros. SSL funciona mediante la creación de un canal de comunicación

cifrado entre el cliente y el servidor, lo que permite que los datos se transmitan de forma segura a través de la red. Para evitar la suplantación de identidad, SSL utiliza certificados digitales para autenticar la identidad del servidor y del cliente.

Además de proporcionar seguridad, SSL también garantiza la integridad de los datos transmitidos a través de la red, asegurando que los datos no sean manipulados o alterados durante la transmisión. SSL es compatible con una amplia variedad de navegadores web y sistemas operativos, lo que lo hace adecuado para su uso en una amplia gama de entornos de red. Aunque SSL ha sido reemplazado por el protocolo de seguridad de transporte (TLS) en versiones más recientes de navegadores y sistemas operativos, el término SSL a menudo se utiliza para referirse a ambos protocolos [29].

Características

- Seguridad: SSL proporciona una capa adicional de seguridad a la conexión en línea, cifrando los datos transmitidos entre el cliente y el servidor.
- Autenticación: SSL utiliza certificados digitales para autenticar la identidad del servidor y del cliente, lo que evita la suplantación de identidad.
- Integridad: SSL garantiza la integridad de los datos transmitidos a través de la red, asegurando que los datos no sean manipulados o alterados durante la transmisión.
- Compatibilidad: SSL es compatible con una amplia variedad de navegadores web y sistemas operativos, lo que lo hace adecuado para su uso en una amplia gama de entornos de red.
- Flexibilidad: SSL se puede utilizar para proteger la transmisión de datos en una amplia variedad de aplicaciones en línea, como transacciones financieras y acceso a sitios web seguros.
- Escalabilidad: SSL puede escalar para admitir un gran número de usuarios y aplicaciones en línea, lo que lo hace adecuado para su uso en entornos empresariales.
- Mejora del rendimiento: SSL también puede mejorar el rendimiento de las aplicaciones en línea, ya que reduce el tiempo de espera para la respuesta del servidor al utilizar una conexión persistente [30].

OpenVPN

OpenVPN es un protocolo de VPN de código abierto que se utiliza para establecer conexiones seguras entre dispositivos en una red de computadoras a través de Internet. Fue creado por James Yonan en 2001 y se ha convertido en uno de los protocolos VPN más populares en todo el mundo debido a su capacidad para utilizar técnicas de criptografía para garantizar la privacidad y seguridad de la transmisión de datos. El funcionamiento de OpenVPN se basa en la creación de un túnel de conexión cifrada entre dos dispositivos a través de Internet, lo que permite que los datos se transmitan de forma segura. La seguridad de los datos se asegura mediante el uso de técnicas de cifrado y autenticación de clave pública.

OpenVPN es compatible con una amplia variedad de sistemas operativos, lo que lo hace accesible para una gran cantidad de usuarios. Además, OpenVPN es altamente configurable y puede adaptarse a las necesidades específicas de la red y del usuario. También cuenta con diversas características de seguridad avanzadas, como la autenticación de dos factores y la autenticación de certificados, lo que lo hace ideal para su uso empresarial y personal [31].

Características

- Es de código abierto: OpenVPN es un protocolo de código abierto, lo que significa que su código fuente es de acceso público y se puede modificar y adaptar a las necesidades específicas de la red o del usuario.
- Es altamente configurable: OpenVPN es altamente configurable, lo que lo hace adecuado para una amplia gama de entornos de red. Puede ser ajustado para adaptarse a las necesidades específicas de la red o del usuario.
- Utiliza técnicas de cifrado y autenticación: OpenVPN utiliza técnicas de cifrado y autenticación para garantizar la seguridad de los datos que se transmiten entre dispositivos.
- Es compatible con varios sistemas operativos: OpenVPN es compatible con varios sistemas operativos, incluyendo Windows, macOS, Linux, Android e iOS.

- Proporciona una conexión segura y privada: OpenVPN permite la creación de un túnel de conexión cifrada entre dos dispositivos a través de Internet, lo que permite la transmisión segura y privada de datos.
- Ofrece características avanzadas de seguridad: OpenVPN cuenta con características avanzadas de seguridad, como la autenticación de dos factores y la autenticación de certificados, que lo hacen muy seguro y confiable para el uso empresarial y personal.
- Es escalable: OpenVPN es escalable, lo que significa que puede manejar una gran cantidad de conexiones simultáneas sin comprometer la velocidad o la seguridad de la conexión.
- Es fácil de usar: OpenVPN es relativamente fácil de usar y configurar, lo que lo hace adecuado para usuarios con diferentes niveles de experiencia técnica [31].

1.2.5.3 Calidad de Servicio (QoS) en túneles VPN

La Calidad de Servicio (QoS) en túneles VPN se define como la habilidad de una red privada virtual para ofrecer un rendimiento constante y óptimo en términos de ancho de banda, latencia, jitter y pérdida de paquetes, a través de un túnel seguro y cifrado que conecta los extremos. La importancia de la QoS radica en que permite la entrega confiable y prioritaria de tráfico crítico, como voz, video y datos sensibles a la latencia, para asegurar una experiencia satisfactoria al usuario y minimizar interrupciones en la comunicación y la productividad. La configuración adecuada de los parámetros de QoS en los dispositivos de red, la implementación de políticas de priorización de tráfico y el monitoreo y ajuste continuo de la QoS son elementos clave para lograr una QoS efectiva en túneles VPN y cumplir con los niveles de servicio acordados [32].

Parámetros

- Ancho de banda: la cantidad de datos que pueden transferirse a través del túnel VPN en un período de tiempo determinado.
- Latencia: el tiempo que tarda un paquete de datos en viajar desde el dispositivo de origen al dispositivo de destino a través del túnel VPN.

- Jitter: la variación en el tiempo de llegada de los paquetes de datos a través del túnel VPN.
- Pérdida de paquetes: el porcentaje de paquetes de datos que se pierden durante la transmisión a través del túnel VPN.
- Priorización de tráfico: la capacidad de dar prioridad a ciertos tipos de tráfico, como voz o video, sobre otros tipos de tráfico, como correo electrónico o descargas de archivos.
- Control de congestión: la capacidad de detectar y manejar la congestión en la red, para evitar la pérdida de paquetes y garantizar una transmisión de datos confiable.
- Seguridad: la capacidad de garantizar la privacidad y la integridad de los datos transmitidos a través del túnel VPN.
- Disponibilidad: la capacidad de mantener el túnel VPN disponible y en funcionamiento de manera confiable, para garantizar una conectividad constante [32].

1.2.6 Encapsulamiento UDP

La Encapsulación UDP (User Datagram Protocol) es un método de empaquetamiento de datos de red en el que los datos se colocan dentro de un datagrama UDP para su transmisión a través de una red. El UDP es un protocolo de capa de transporte en el modelo OSI (Open Systems Interconnection) que se utiliza comúnmente para aplicaciones que requieren una transmisión rápida y eficiente de datos, como la transmisión de video y voz en tiempo real.

La información generada en la capa de aplicación se transmite en bloques discretos de bytes al protocolo de la capa de transporte. En el caso de UDP, estos datos se encapsulan con un encabezado propio, pero en lugar de denominarlos segmentos como en TCP, se les conoce como datagramas. Los datagramas se envían a la capa de red, donde se agrega otro encabezado y se convierten en paquetes. Estos paquetes son enviados a la capa de enlace de datos, donde se convierten en tramas. Todo este proceso se puede visualizar en la figura 13 [33].

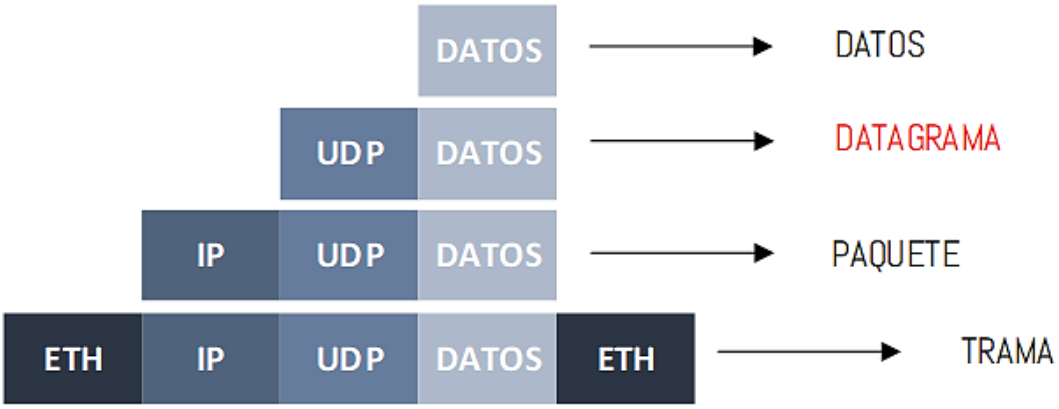


Figura 12. Encapsulamiento UDP [33].

1.3 Objetivos

1.3.1 Objetivo General

Diseñar el sistema de comunicación y videovigilancia basado en túneles VPN para la integración de las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en el Ecuador.

1.3.2 Objetivos Específicos

- Analizar la situación actual de la red de comunicación de la Cooperativa de ahorro y crédito vencedores de Tungurahua.
- Determinar el correcto protocolo de interconexión VPN que ofrezca una comunicación segura entre la matriz y las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua.
- Seleccionar los equipos de red para la implementación del sistema de comunicaciones basado en túnel VPN entre la matriz y las sucursales de la Cooperativa.
- Implementación de un prototipo del sistema de comunicación y video vigilancia basado en túneles VPN entre la matriz y la sucursal principal de Quisapincha de la Cooperativa de ahorro y crédito vencedores de Tungurahua.

CAPÍTULO II

METODOLOGÍA.

2.1 Materiales

Para llevar a cabo este proyecto de investigación, se utilizaron diversas herramientas que permitieron obtener información de diversas fuentes, como libros, artículos científicos y proyectos similares al tema en cuestión. Además, se contó con el asesoramiento de profesionales en el área investigada, y se emplearon herramientas de software y hardware para diseñar el sistema de comunicación y videovigilancia basado en túneles VPN. Todo ello con el objetivo de integrar las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en Ecuador.

2.2 Métodos

2.2.1 Modalidad de Investigación

Este proyecto tuvo como objetivo diseñar un sistema de comunicación y videovigilancia basado en túneles VPN para integrar las diferentes sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en el Ecuador. Para llevar a cabo este proyecto, se utilizaron las siguientes modalidades de investigación:

2.2.1.1 Investigación de Campo

El desarrollo del proyecto se llevó a cabo en dos lugares importantes de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua. El primer lugar fue en la sede principal de la Cooperativa, donde se realizó la planificación, diseño y pruebas iniciales del sistema de comunicación y videovigilancia basado en túneles VPN. El segundo lugar fue en la sucursal principal de la Cooperativa, ubicada en Quisapincha, donde se implementó el sistema y se realizaron pruebas finales para asegurar su correcto funcionamiento.

2.2.1.2 Investigación Bibliográfica

Para la realización de este proyecto de investigación se empleó una metodología basada en la investigación bibliográfica, que consistió en la recolección de información

científica relacionada con el tema de estudio. Esta investigación se llevó a cabo principalmente a través del uso de revistas científicas, artículos científicos, publicaciones y proyectos de titulación de repositorios públicos y privados desarrollados en los últimos años. Todos estos recursos estuvieron vinculados a la conexión de redes mediante túneles VPN y fueron utilizados para obtener información relevante para el desarrollo del proyecto.

2.2.1.3 Investigación Experimental

Se llevaron a cabo diversas pruebas para evaluar el rendimiento y la eficacia del sistema de comunicación y videovigilancia basado en túneles VPN para la integración de las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en el Ecuador. Estas pruebas permitieron verificar la funcionalidad del sistema y asegurarse de que cumpliera con los requisitos y especificaciones previamente establecidos.

2.2.2 Población y Muestra

Para este proyecto de investigación no fue necesario realizar una muestra o tomar en cuenta una población en particular, porque se enfocó en el diseño del sistema de comunicación y videovigilancia de la matriz y la sucursal principal de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua.

2.2.3 Recolección de información

La recolección de información se llevó a cabo mediante una investigación exhaustiva de diversas fuentes, tales como libros, revistas científicas, recursos en línea y proyectos de titulación relacionados con los parámetros relevantes a considerar en la implementación de túneles VPN. Además, se recurrió a documentos oficiales proporcionados por los fabricantes de dispositivos de red para garantizar una configuración adecuada

2.2.4 Procesamiento y análisis de datos

Se llevó a cabo el procesamiento de información recopilada en antecedentes investigativos relacionados al sistema de comunicación y videovigilancia basado en

túneles VPN, a partir de artículos científicos que presentaran similitud tanto teórica como práctica. Se hizo una segmentación de la información considerando su utilidad completa para el marco teórico, descartando información redundante o que no contara con una fuente bibliográfica confiable. Se siguieron los siguientes pasos:

- Revisión de la información recopilada
- Análisis de la información referente a sistemas de comunicación mediante túneles VPN.
- Planteamiento de la propuesta de solución.
- Confirmación de los datos obtenidos a través de diversas pruebas de funcionamiento.

2.2.5 Desarrollo del proyecto

Para llevar a cabo el proyecto de integración de las diferentes sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en el Ecuador mediante túneles VPN, se siguieron una serie de etapas para garantizar su correcto funcionamiento. Se realizó una investigación exhaustiva de los parámetros físicos y geográficos de las zonas donde se ubican las sucursales, identificando los elementos necesarios para su implementación y analizando su funcionamiento. Se llevó a cabo el diseño del sistema de comunicación y videovigilancia, eligiendo la tecnología adecuada para asegurar la calidad y seguridad de la información transmitida. Finalmente, se realizaron pruebas exhaustivas para verificar el correcto funcionamiento del sistema. Los pasos fueron los siguientes:

1. Análisis de la red de comunicación actual de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua
2. Análisis de los equipos con el cual cuenta actualmente la Cooperativa De Ahorro y Crédito Vencedores De Tungurahua.
3. Determinación del protocolo a utilizar en la red VPN para la interconexión entre la matriz y las sucursales que posee en el Ecuador la institución financiera
4. Selección de los equipos de red faltantes que permita realizar la implementación del sistema de comunicación, monitoreo y comunicación remota mediante túneles VPN

5. Comparación de equipos entre características, análisis de disponibilidad, garantía de tráfico de datos, soporte de protocolos de redes VPN y precios de los equipos a utilizarse
6. Comparación de equipos entre características, análisis de disponibilidad, garantía de tráfico de datos, soporte de protocolos de redes VPN y precios de los equipos a utilizarse
7. Diseño del sistema de comunicación mediante túneles VPN
8. Programación del sistema de comunicación entre sucursales mediante la aplicación de túneles VPN
9. Pruebas de funcionamiento del sistema de comunicaciones.
10. Corrección de posibles errores.
11. Elaboración del informe final del proyecto

CAPÍTULO III

RESULTADOS Y DISCUSIÓN.

CLÁUSULA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

La Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en Ecuador, al ser una institución financiera, no es posible presentar toda la información que se utilizó para el desarrollo del presente trabajo de Titulación, esto es por seguridad de la Cooperativa, y para evitar posibles ataques cibernéticos que puedan causar daños a sus servidores y/o pérdidas a la institución.

Toda la información generada y publicada en este documento es autorizada y supervisada por la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua. En caso de que la información brindada se utilice con fines de perjudicar a la Cooperativa, la institución financiera tomará acciones legales.

3.1 Análisis y discusión de los resultados

La implementación de un sistema de comunicación y video vigilancia basado en túneles VPN para la integración de las sucursales de la Cooperativa de Ahorro y Crédito (COAC) Vencedores de Tungurahua en Ecuador, permite una comunicación segura y confiable entre las diferentes sucursales, lo que mejora el rendimiento y la eficiencia de los procesos internos de la organización. Además, este sistema proporciona un alto nivel de seguridad en la transferencia de datos y una reducción significativa de los costos de comunicación. La integración de las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua a través de una red segura y confiable permite una mejor gestión de los recursos y la optimización de los procesos internos. El sistema de video vigilancia también proporciona una mayor seguridad en las instalaciones de la Cooperativa, lo que permite prevenir y detectar posibles delitos o actividades sospechosas.

3.2 Desarrollo de la propuesta

3.2.1 Situación actual de la red de los sistemas de comunicación de las sucursales de la Cooperativa Vencedores de Tungurahua.

El proceso de comunicación actual entre la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua y cada una de sus diferentes sucursales ubicadas en las distintas ciudades del Ecuador, es a través del proveedor de servicios de Internet NETLIFE, la institución financiera no cuenta con un red o sistema propio de comunicación, de manera que se ven forzado a tener convenio con otras empresas que ofrezcan este servicio, en este caso la institución financiera tiene un convenio con la operadora claro, pagando planes de algunos empleados de la institución, es por esta razón que los gastos por telefonía son elevados, además, la cooperativa Vencedores carece del sistema de monitoreo constate de las cámaras de video vigilancia.

El objetivo es contar con una sala de monitoreo en la oficina matriz, así como un sistema de comunicación VoIP privado mediante la implementación de un túnel VPN para garantizar una transmisión de datos segura y confiable.

Para llevar a cabo este proyecto y lograr los objetivos planteados, el primer paso fue analizar la situación y estado actual de los sistemas de comunicación en cada sucursal que forma parte de la Cooperativa Vencedores de Tungurahua.

A continuación, se detallan los elementos que conforman los equipos y puntos de red en cada una de ellas.

Localización

En la siguiente tabla, se muestra la ubicación de la Cooperativa de Ahorro y crédito Vencedores de Tungurahua en las distintas ciudades del Ecuador y su dirección en cada una de ellas.

Tabla 7. Ubicación de la matriz y sucursales de la Cooperativa Vencedores

COOPERATIVA DE AHORRO Y CRÉDITO VENCEDORES		**DIRECCIÓN**
Matriz	Ambato	Calle Simón Bolívar 09-35
Sucursal 1	Quisapincha	Calle 10 de agosto y Gonzáles Suárez
Sucursal 2	Quito	Calle Luis Pallares N 5-637

Sucursal 3	Latacunga	Calle 2 de mayo y Belisario Quevedo
Sucursal 4	Saquisili	Calle Simón Bolívar y Pichincha
Sucursal 5	Riobamba	Calle Juan Montalvo y Villarroel

Elaborado por: El Investigador

Datos Generales

En la tabla 8, se detallan los datos generales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua oficina matriz.

Tabla 8. Datos generales oficina matriz

Cantón	Ambato
Posee servicio de internet	Si
Proveedor	Netfile
Última Milla	Fibra
Sistema de video vigilancia	Si
Telefonía IP	Si
Puntos de red	32
Características de la red	Cableado e inalámbrico

Elaborado por: El Investigador

En la tabla 9, se detallan los datos generales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua sucursal principal Quisapincha.

Tabla 9. Datos generales sucursal Quisapincha

Cantón	Ambato
Posee servicio de internet	Si
Proveedor	Netfile
Última Milla	Fibra
Sistema de video vigilancia	Si
Telefonía IP	Si
Puntos de red	27
Características de la red	Cableado e inalámbrico

Elaborado por: El Investigador

En la tabla 10, se detallan los datos generales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua sucursal Riobamba.

Tabla 10. Datos generales sucursal Riobamba

Cantón	Ambato
Posee servicio de internet	Si
Proveedor	Netfile
Última Milla	Fibra
Sistema de video vigilancia	Si
Telefonía IP	Si
Puntos de red	17
Características de la red	Cableado e inalámbrico

Elaborado por: El Investigador

En la tabla 11, se detallan los datos generales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua sucursal Latacunga.

Tabla 11. Datos generales sucursal Latacunga

Cantón	Latacunga
Posee servicio de internet	Si
Proveedor	Netfile
Última Milla	Fibra
Sistema de video vigilancia	Si
Telefonía IP	Si
Puntos de red	20
Características de la red	Cableado e inalámbrico

Elaborado por: El Investigador

En la tabla 12, se detallan los datos generales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua sucursal Saquisili.

Tabla 12. Datos generales sucursal Saquisili

Cantón	Saquisili
Posee servicio de internet	Si
Proveedor	CNT
Última Milla	Fibra
Sistema de video vigilancia	Si
Telefonía IP	Si
Puntos de red	20
Características de la red	Cableado e inalámbrico

Elaborado por: El Investigador

En la tabla 13, se detallan los datos generales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua sucursal Quito.

Tabla 13. Datos generales sucursal Quito

Cantón	Guamaní
Posee servicio de internet	Si
Proveedor	Netlife
Última Milla	Fibra
Sistema de video vigilancia	Si
Telefonía IP	Si
Puntos de red	18
Características de la red	Cableado e inalámbrico

Elaborado por: El Investigador

Datos de Equipos

A continuación, en la siguiente tabla, se describen los equipos de red que utiliza la oficina matriz, con sus diferentes características técnicas.

Tabla 14. Equipos de red de COAC Vencedores Matriz-Ambato

COAC VENCEDORES MATRIZ (AMBATO)				
EQUIPOS DE RED				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Router	1	Mikrotik	CRS326-24GZSTRM	Capa 2 24 puertos Ethernet Soporte 4K VLANs simultáneas Puerto seguro
Switch	1	Cisco	SLM224PT-NA	ADMINISTRABLE. 12 puertos PoE.

Elaborado por: El Investigador

En la siguiente tabla, se describen los equipos de Telefonía IP que se manejan en cada área de trabajo como es la central telefónica, operadora y teléfonos IP.

Tabla 15. Equipos de telefonía IP

COAC VENCEDORES MATRIZ (AMBATO)				
EQUIPOS TELÉFONO IP				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Central telefónica	1	GRANDSTREAM	UCM 6202-2	Protocolos de Red TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE. Códecs de Video H.264, H.263, H263+.
Operadora	1	GRANDSTREAM	GXP-1628	Dos puertos de red Ethernet. 2 cuentas sip. TLS/SRTP/HTTPS para seguridad.
Teléfonos IP	11	GRANDSTREAM	GXP-1610	Conferencia de hasta 3 vías. TLS/SRTP/HTTPS para seguridad

Elaborado por: El Investigador

Los equipos de video vigilancia que utiliza la sucursal se detallan en la tabla siguiente, con sus debidas especificaciones técnicas.

Tabla 16. Equipos de video vigilancia de la oficina Matriz

COAC VENCEDORES MATRIZ (AMBATO)				
EQUIPOS VIDEO VIGILANCIA				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
DVR	1	HIKVISION	DS-7332HUHI-K4	32 canales de vídeo TURBOHD + 16 canales IP. Soporta Hik-Connect (P2P).
Cámara domo	18	HIKVISION	DS-2CE56D0T-IRPF	Salida Analógica HD, hasta 1080p. Alcance de Infrarrojo hasta 20 mtrs.
Cámara tubo	2	HIKVISION	DS-2CE16D3T-IT3F	IP67. Alcance de Infrarrojo hasta 40 mtrs. Salida Analógica HD, hasta 1080p.
Cámara domo (IP)	6	HIKVISION	DS-2CD1327G0-L	Imagen a Color 24/7 PoE Lente 2.8 mm. 2 megapíxeles

Elaborado por: El Investigador

Se describen los equipos de red de la sucursal principal Quisapincha en la siguiente tabla.

COAC VENCEDORES SUCURSAL PRINCIPAL (QUISAPINCHA)

Tabla 17. Equipos de red de COAC Vencedores Quisapincha

COAC VENCEDORES SUCURSAL PRINCIPAL (QUISAPINCHA)				
EQUIPOS DE RED				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Router	1	Mikrotik	CRS326-24GZSTRM	Capa 2 24 puertos Ethernet Soporte 4K VLANs simultáneas Puerto seguro

Elaborado por: El Investigador

En la siguiente tabla se muestran los equipos de Telefonía IP de la sucursal principal Quisapincha.

Tabla 18. Equipos de telefonía IP

COAC VENCEDORES SUCURSAL PRINCIPAL (QUISAPINCHA)				
EQUIPOS TELÉFONO IP				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Central telefónica	1	GRANDSTREAM	UCM 6202-2	Protocolos de Red TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE. Códecs de Video H.264, H.263, H263+.
Operadora	1	GRANDSTREAM	GXP-1628	Dos puertos de red Ethernet. 2 cuentas sip. TLS/SRTP/HTTPS para seguridad.
Teléfonos IP	7	GRANDSTREAM	GXP-1610	Conferencia de hasta 3 vías. TLS/SRTP/HTTPS para seguridad

Elaborado por: El Investigador

Los equipos de video vigilancia que utiliza la sucursal de Quisapincha, se detallan a continuación, con sus debidas especificaciones técnicas.

Tabla 19. Equipos de video vigilancia de la sucursal Quisapincha

COAC VENCEDORES SUCURSAL PRINCIPAL (QUISAPINCHA)				
EQUIPOS VIDEO VIGILANCIA				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
DVR	1	HIKVISION	DS-7332HQHI-K4	32 canales de vídeo TURBOHD + 16 canales IP. Soporta Hik-Connect (P2P).
Cámara domo	10	HIKVISION	DS-2CE56D0T-IRPF	Salida Analógica HD, hasta 1080p. Alcance de Infrarrojo hasta 20 mtrs.
Cámara tubo	2	HIKVISION	DS-2CE16D3T-IT3F	IP67. Alcance de Infrarrojo hasta 40 mtrs. Salida Analógica HD, hasta 1080p.

Elaborado por: El Investigador

Existen 19 puntos de red que la sucursal principal Quisapincha abastece los cuales, se enumeran en la siguiente tabla.

Tabla 20. Puntos de red de la sucursal principal Vencedores Quisapincha

Lista	Puntos de red
1	RED ATENCION AL CLIENTE
2	RED IMPRESIRA ATENCION AL CLIENTE
3	RED CAJAS 1
4	RED CAJAS 2
5	RED OFICINA FRENTE A SISTEMAS
6	RED MAQUINA ELIZA
7	RED IMPRESORA ELIZA
8	RED PEDRO CHUQUIANA
9	RED EDISSON APUPALO
10	RED VICTOR TUSA
11	RED EDIZON SOGSO
12	RED SISTEMAS
13	RED GERENCIA
14	RED AUDITORIO
15	RED ARCHIVO
16	RED CONTABILIDAD
17	RED ROUTER
18	RED SERVIDOR 1
19	RED SERVIDOR 2

Elaborado por: El Investigador

COAC VENCEDORES SUCURSAL QUITO

Tabla 21. Equipos de red de COAC Vencedores Sucursal-Quito

COAC VENCEDORES SUCURSAL QUITO				
EQUIPOS DE RED				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Router	1	Mikrotik	CRS326-24GZSTRM	Capa 2 24 puertos Ethernet Soporte 4K VLANs simultáneas Puerto seguro

Elaborado por: El Investigador

En la siguiente tabla, se describen los equipos de Telefonía IP de la sucursal principal Quito

Tabla 22. Equipos de telefonía IP

COAC VENCEDORES SUCURSAL QUITO				
EQUIPOS TELÉFONO IP				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Central telefónica	1	GRANDSTREAM	UCM 6202-2	Protocolos de Red TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE. Códecs de Video H.264, H.263, H263+.
Teléfonos IP	5	GRANDSTREAM	GXP-1610	Conferencia de hasta 3 vías. TLS/SRTP/HTTPS para seguridad

Elaborado por: El Investigador

Los equipos de video vigilancia que utiliza la sucursal de Quito, se detallan en la tabla 23 con sus debidas especificaciones técnicas.

Tabla 23. Equipos de video vigilancia de la sucursal Quito

COAC VENCEDORES SUCURSAL QUITO				
EQUIPOS VIDEO VIGILANCIA				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
NVR	1	HIKVISION	DS-7608NI-K1/8P	Protocolo De Red TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMPHTTP, HTTPS
Cámaras domo	4	HIKVISION	DS-2CD1123GOE-I	2 Megapixel. Infrarrojo: 30 mts
Cámaras tubo	2	HIKVISION	DS-2CE16D3T-IT3F	2 Megapixel. IP67

Elaborado por: El Investigador

Existen 9 puntos de red que la sucursal principal Quito abastece los cuales se describen a continuación.

Tabla 24. Puntos de red de la sucursal principal Vencedores Quito

Lista	Puntos de red
1	RED ATENCION AL CLIENTE 2 PUNTOS
2	RED IMPRESORA ATENCION AL CLIENTE
3	RED CAJAS 1
4	RED CAJAS 2
5	RED ASESORES 2 PUNTOS
6	RED ASESOR 1 PUNTO
7	RED JEFE DE AGENCIA
8	RED ASESORES

Elaborado por: El Investigador

La siguiente figura, se puede ver el rack instalado en la sucursal Quito con los diferentes dispositivos como es el DVR, router Mikrotik, UCM 6202, entre otros.

Figura 13. Rack instalado sucursal Quito

COAC VENCEDORES SUCURSAL LATACUNGA

Tabla 25. Equipos de red de COAC Vencedores Sucursal-Latacunga

COAC VENCEDORES SUCURSAL LATACUNGA				
EQUIPOS DE RED				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Router	1	Mikrotik	CRS326-24GZSTRM	Capa 2 24 puertos Ethernet Soporte 4K VLANs simultáneas

Elaborado por: El Investigador

En la tabla 26, se describen los equipos de Telefonía IP de la sucursal Latacunga

Tabla 26. Equipos de telefonía IP

COAC VENCEDORES SUCURSAL LATACUNGA				
EQUIPOS TELÉFONO IP				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Central telefónica	1	GRANDSTREAM	UCM 6202-2	Protocolos de Red TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE. Códecs de Video H.264, H.263, H263+.
Teléfonos IP	4	GRANDSTREAM	GXP-1610	Conferencia de hasta 3 vías. TLS/SRTP/HTTPS para seguridad

Elaborado por: El Investigador

Los equipos de video vigilancia que utiliza la sucursal de Latacunga, se detallan en la tabla 27 con sus debidas especificaciones técnicas.

Tabla 27. Equipos de video vigilancia de la sucursal Latacunga

COAC VENCEDORES SUCURSAL LATACUNGA				
EQUIPOS VIDEO VIGILANCIA				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
NVR	1	HIKVISION	DS-7608NI-K1/8P	Protocolo De Red TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMPHTTP, HTTPS
Cámaras domo	6	HIKVISION	DS-2CD1123GOE-I	2 Megapixel. Infrarrojo: 30 mts
Cámaras tubo	2	HIKVISION	DS-2CE16D3T-IT3F	2 Megapixel. IP67

Elaborado por: El Investigador

Existen 10 puntos de red que la sucursal Latacunga abastece, los cuales, se describen en la tabla 28.

Tabla 28. Puntos de red de la sucursal principal Vencedores Latacunga

Lista	Puntos de red
1	RED ATENCIÓN AL CLIENTE 2 PUNTOS
2	RED IMPRESORA ATENCIÓN AL CLIENTE
3	RED CAJAS 1
4	RED CAJAS 2
5	RED ASESORES 2 PUNTOS
6	RED ASESOR
7	RED JEFA DE AGENCIA
8	RED INVERSIONES 2P

Elaborado por: El Investigador

La siguiente figura, muestra el rack instalado en la sucursal Latacunga con los diferentes dispositivos como es el DVR, router Mikrotik, fuente de alimentación, entre otros.

Figura 14. Rack instalado sucursal Latacunga

COAC VENCEDORES SUCURSAL SAQUISILI

Tabla 29. Equipos de red de COAC Vencedores Sucursal-Saquisili

COAC VENCEDORES SUCURSAL SAQUISILI				
EQUIPOS DE RED				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Router	1	Mikrotik	CRS326-24GZSTRM	24 puertos Soporte 4K VLANs simultáneas

Elaborado por: El Investigador

En la tabla 30, se describen los equipos de Telefonía IP de la sucursal Saquisili

Tabla 30. Equipos de telefonía IP

COAC VENCEDORES SUCURSAL SAQUISILI				
EQUIPOS TELÉFONO IP				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Central telefónica	1	GRANDSTREAM	UCM 6202-2	Protocolos de Red TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE. Códecs de Video H.264, H.263, H263+.
Teléfonos IP	4	GRANDSTREAM	GXP-1610	Conferencia de hasta 3 vías. TLS/SRTP/HTTPS para seguridad

Elaborado por: El Investigador

Los equipos de video vigilancia que utiliza la sucursal de Saquisili, se detallan en la tabla 31 con sus debidas especificaciones técnicas.

Tabla 31. Equipos de video vigilancia de la sucursal Saquisili

COAC VENCEDORES SUCURSAL SAQUISILI				
EQUIPOS VIDEO VIGILANCIA				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
NVR	1	HIKVISION	DS-7608NI-Q2/8P	Protocolo De Red TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, HTTPS
Cámaras domo	4	HIKVISION	DS-2CD1123GOE-I	2 Megapixel. Infrarrojo: 30 mts
Cámaras tubo	2	HIKVISION	DS-2CE16D3T-IT3F	2 Megapixel. IP67

Elaborado por: El Investigador

Existen 10 puntos de red que la sucursal Saquisili abastece los cuales se describen en la tabla 32.

Tabla 32. Puntos de red de la sucursal principal Vencedores Saquisili

Lista	Puntos de red
1	RED ATENCIÓN AL CLIENTE 2 PUNTOS
2	RED IMPRESORA ATENCIÓN AL CLIENTE
3	RED CAJAS 1
4	RED CAJAS 2
5	RED ASESORES 2 PUNTOS
6	RED ASESOR 1 PUNTO
7	RED JEFA DE AGENCIA
8	RED JUNTO JEFA DE AGENCIA

Elaborado por: El Investigador

La siguiente figura, representa el rack de la COAC VENCEDORES SUCURSAL SAQUISILI, funcionando con los diferentes equipos que lo conforma.

Figura 15. Rack instalado Sucursal Saquisili

COAC VENCEDORES SUCURSAL RIOBAMBA

Tabla 33. Equipos de red de COAC Vencedores Sucursal-Riobamba

COAC VENCEDORES SUCURSAL RIOBAMBA				
EQUIPOS DE RED				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Router	1	Mikrotik	CRS326-24GZSTRM	Capa 2 24 puertos Ethernet Soporte 4K VLANs simultáneas Puerto seguro

Elaborado por: El Investigador

En la tabla 34, se describen los equipos de Telefonía IP de la sucursal Riobamba

Tabla 34. Equipos de telefonía IP

COAC VENCEDORES SUCURSAL RIOBAMBA				
EQUIPOS TELÉFONO IP				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
Central telefónica	1	GRANDSTREAM	UCM 6202-2	Protocolos de Red TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE. Códecs de Video H.264, H.263, H263+.
Teléfonos IP	3	GRANDSTREAM	GXP-1610	Conferencia de hasta 3 vías. TLS/SRTP/HTTPS para seguridad

Elaborado por: El Investigador

Los equipos de video vigilancia que utiliza la sucursal de Riobamba, se detallan en la tabla 35 con sus debidas especificaciones técnicas.

Tabla 35. Equipos de video vigilancia de la sucursal Riobamba

COAC VENCEDORES SUCURSAL RIOBAMBA				
EQUIPOS VIDEO VIGILANCIA				
Dispositivo	**Cantidad**	**Marca**	**Modelo**	**Características**
NVR	1	HIKVISION	DS-7608NI-K1/8P	Protocolo De Red TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMPHTTP, HTTPS
Cámaras domo	6	HIKVISION	DS-2CD1123GOE-I	2 Megapixel. Infrarrojo: 30 mts
Cámaras tubo	2	HIKVISION	DS-2CE16D3T-IT3F	2 Megapixel. IP67

Elaborado por: El Investigador

Existen 10 puntos de red que la sucursal Riobamba abastece, los cuales, se describen en la tabla 36.

Tabla 36. Puntos de red de la sucursal principal Vencedores Riobamba

Lista	Puntos de red
1	RED ATENCIÓN AL CLIENTE 2 PUNTOS
2	RED IMPRESORA ATENCIÓN AL CLIENTE
3	RED CAJAS 1
4	RED CAJAS 2
5	RED ASESORES 2 PUNTOS
6	RED ASESOR 1 PUNTO
7	RED JEFA DE AGENCIA
8	RED JUNTO JEFA DE AGENCIA

Elaborado por: El Investigador

La figura 17, representa el rack de la COAC VENCEDORES SUCURSAL RIOBAMBA, funcionando con los diferentes equipos que lo conforma.

Figura 16. Rack instalado Sucursal Riobamba

Elaborado por: El Investigador

ESQUEMA GENERAL DE LA RED ACTUAL DE LA COOPERATIVA DE AHORRO Y CREDTO VENCEDORES DE TUNGURAHUA

En la figura 17, representa el esquema de la red actual de la Cooperativa Vencedores en el cual se puede observa que la oficina matriz y las sucursales cuentan ya instaladas con routers mikrotik, cámaras de video vigilancia y telefonía IP. Pero estos sistemas solo funcionan de manera interna para cada oficina.

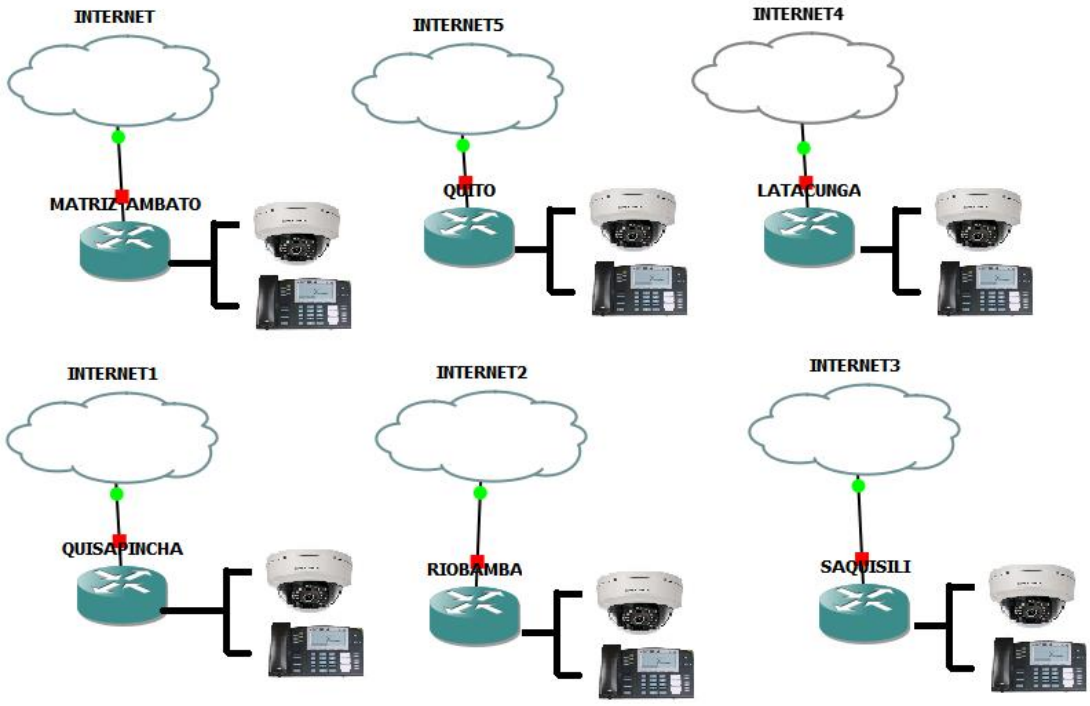


Figura 17. Esquema red actual Cooperativa Vencedores

Elaborado por: El Investigador

3.2.2 Diseño del sistema de comunicación y video vigilancia en túneles VPNs.

En la tabla 37, se detallan los parámetros como la IP pública, IP LAN, puerto y protocolo que se debe utilizar para la configuración de los router y crear los túneles VPNs utilizando el protocolo IPSec. La red propuesta de puede ver en el Anexo A.

Tabla 37. Parámetros establecidos para VPNs de la cooperativa

	IP Pública	IP LAN	PUERTO	Protocolo
Matriz Ambato	200.24.139.2	192.168.10.1	500	UDP

Sucursal Quisapincha	186.3.45.138	192.168.20.1	500	UDP
Sucursal Riobamba	192.168.255.253	192.168.30.1	500	UDP
Sucursal Latacunga	172.20.18.150	192.168.40.1	500	UDP
Sucursal Quito	192.135.250.10	192.168.50.1	500	UDP
Sucursal Saquisili	192.31.7.11	192.168.60.1	500	UDP

Elaborado por: El Investigador

Para la configuración del router Mikrotik es necesario descargar la imagen ISO oficial desde su página web. Esta imagen se carga en GNS3 para permitir la utilización de un router Mikrotik como se muestra en la figura 18.

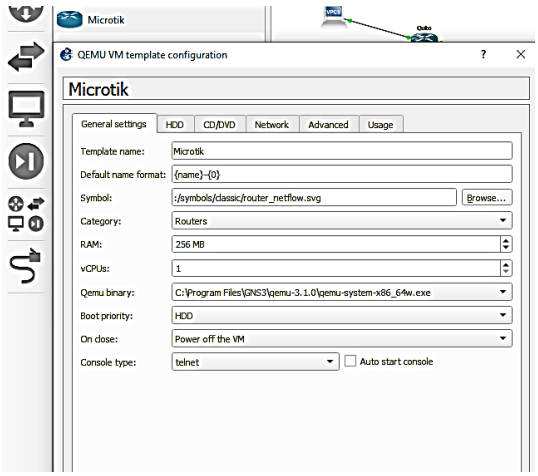


Figura 18. Configuración router Mikrotik en GNS3

Elaborado por: El Investigador

En esta simulación, se representa la red propuesta para la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua, la cual incluye una matriz ubicada en Ambato y sucursales en Riobamba, Saquisilí, Latacunga y Quito, como se visualiza en la figura 19.

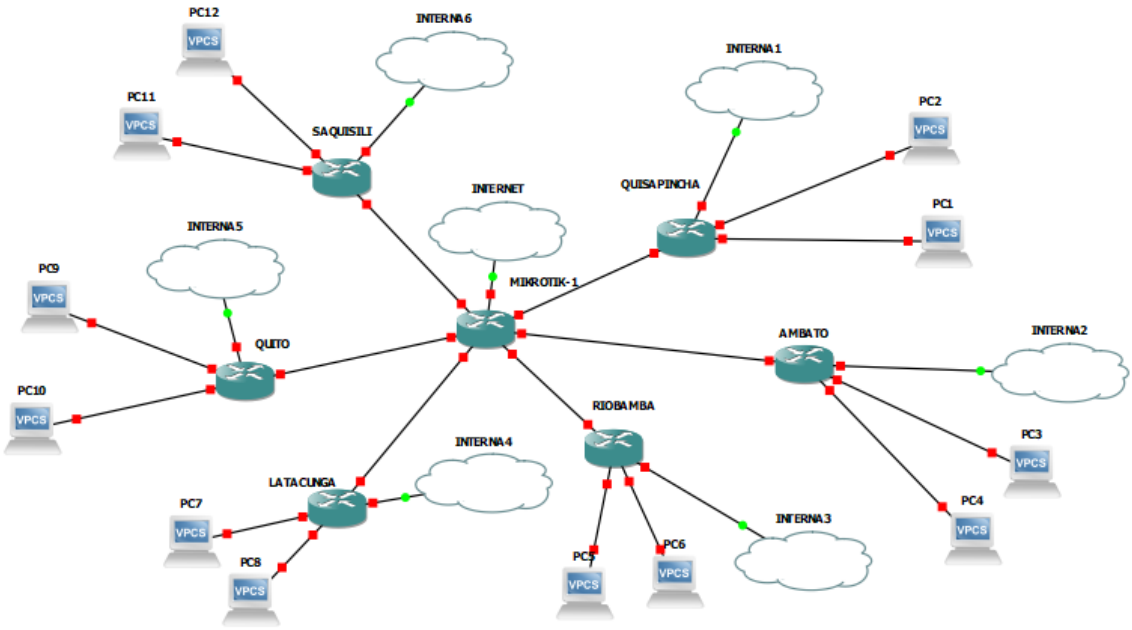


Figura 19. Redes VPNs propuesta para la Cooperativa

Elaborado por: El Investigador

Se establece la comunicación LAN en la matriz como se ve en la figura 20.

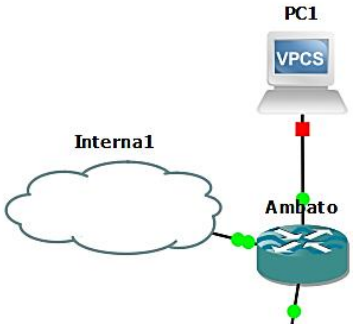


Figura 20. Red LAN matriz Ambato

Elaborado por: El Investigador

Se configura la red LAN para la sucursal Riobamba, en el cual cuenta con la conexión VPN para a interconexión como las demás sucursales, como se visualiza en la figura 21. La programación se puede visualizar en el Anexo B. Donde configuramos el puerto a utilizar, el protocolo, las direcciones públicas, direcciones LAN y la configuración de la NAT.

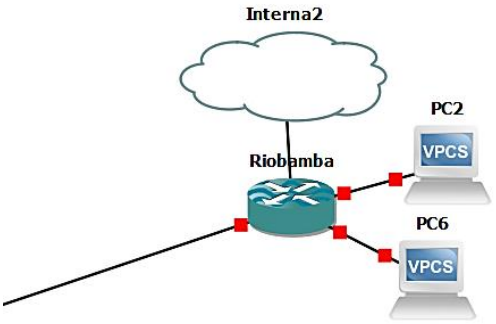


Figura 21. Red LAN sucursal Riobamba

Elaborado por: El Investigador

Se configura la red LAN Quisapincha, de igual forma su VPN para la interconexión con las demás sucursales, como se representa en la figura 22. Su programación se puede observar en el Anexo C. Donde configuramos el puerto a utilizar, el protocolo, las direcciones públicas, direcciones LAN y la configuración de la NAT.

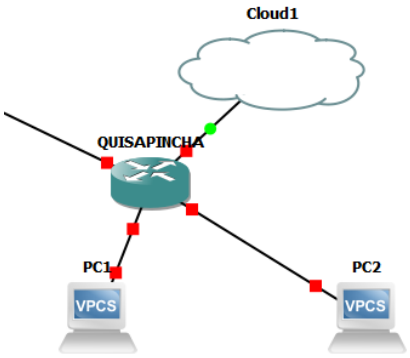


Figura 22. Red LAN sucursal Quisapincha

Elaborado por: El Investigador

Se configura la red LAN Saquisili, de igual forma su VPN para la interconexión con las demás sucursales, como se representa en la figura 22. Su programación se puede observar en el Anexo D. Donde configuramos el puerto a utilizar, el protocolo, las direcciones públicas, direcciones LAN y la configuración de la NAT.

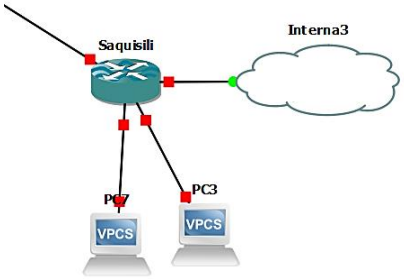


Figura 23. Red LAN sucursal Saquisilí

Elaborado por: El Investigador

Se configura la red LAN para la sucursal Latacunga, de igual forma su VPN con el fin de establecer comunicación con las demás sucursales, como se visualiza en la figura 23. Su programación se puede observar en el Anexo E. Donde configuramos el puerto a utilizar, el protocolo, las direcciones públicas, direcciones LAN y la configuración de la NAT.

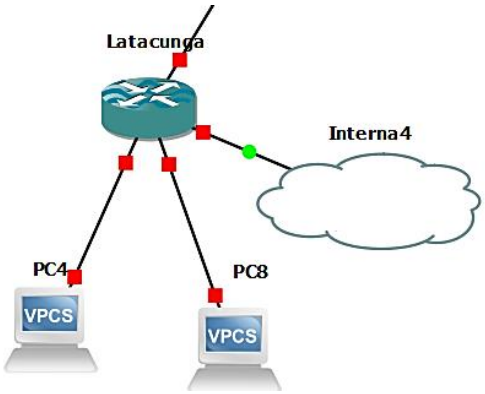


Figura 24. Red LAN Latacunga

Elaborado por: El Investigador

Se configura la red LAN para la sucursal Quito, de igual manera su VPN para establecer comunicación con las sucursales de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua, como se visualiza en la figura 24. Su programación se puede observar en el Anexo F. Donde configuramos el puerto a utilizar, el protocolo, las direcciones públicas, direcciones LAN y la configuración de la NAT.

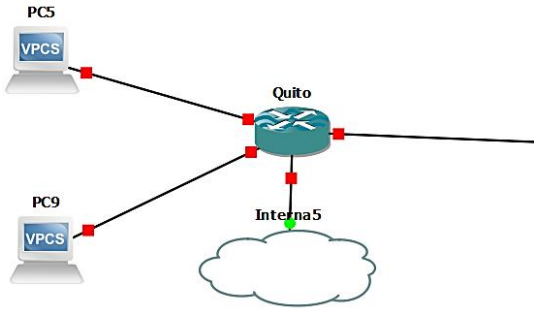


Figura 25. Red LAN Quito

Elaborado por: El Investigador

En la simulación realizada que se visualiza en la figura 25, se ha realizado la programación en los 5 sitios, cada sitio posee un router y como terminal una PC. Por tanto, terminada la configuración de los sitios se puede observar que se ha establecido la comunicación entre las sucursales y la sede principal.

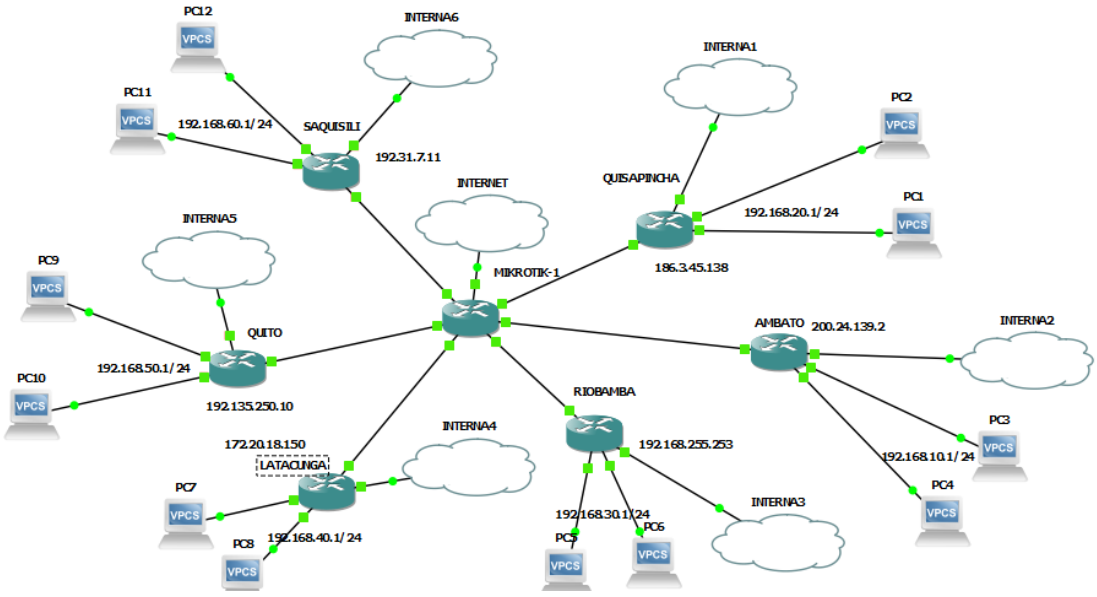


Figura 26. Comunicación VPNs establecida entre los sitios

Elaborado por: El Investigador

El sistema de comunicación simulado en GNS3, permite tener comunicación entre los 5 sitios como se ve en la figura 27. Es decir, se establece la comunicación entre las distintas sucursales y la matriz donde podemos enviar y recibir información.

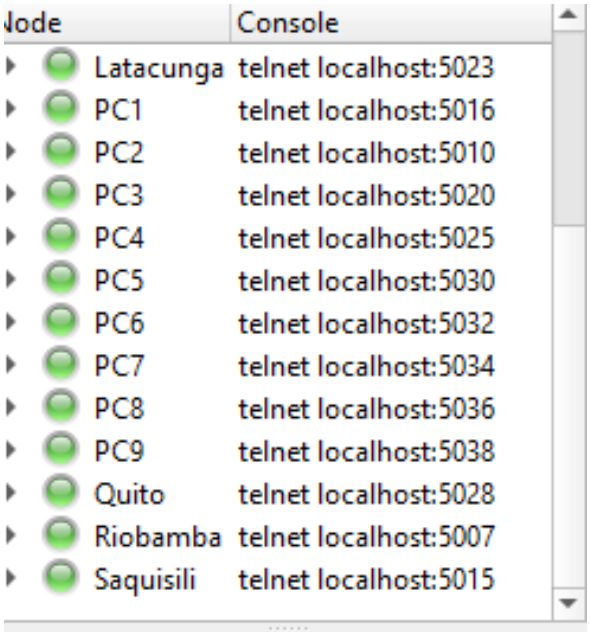


Figura 27. Puntos de conexión en estado conectado

Elaborado por: El Investigador

3.2.3 Configuración y establecimiento de los equipos de comunicación

En la tabla 37 se detalla los parámetros necesarios para la configuración de los túneles VPN utilizando el protocolo IPSec, para lo cual es necesario una IP pública estática, y la IP LAN en diferentes segmentos o subredes, además el protocolo UDP que permite la transmisión de audio y video.

Tabla 38. Parámetros para la configuración de los router Mikrotik

	IP Pública	IP LAN	PUERTO	Protocolo
Matriz Ambato	200.24.139.2	192.168.4.0	500	UDP
Sucursal Quisapincha	186.3.45.138	192.168.5.0	500	UDP

Elaborado por: El Investigador

En el proceso de realizar la configuración física se deben tomar en cuenta los diferentes parámetros y características que han sido analizados en los equipos utilizados que en este caso los routers Mikrotik RB2011UiAS-RB, y la central Grandstream UCM 6301. Se puede encontrar el catálogo en el Anexo G y Anexo H respectivamente.

En la tabla 39, se detallan las características principales de los equipos anteriormente mencionados, por tanto, estos equipos son utilizados para la implementación de este proyecto.

Tabla 39. Características Mikrotik Mikrotik RB2011UiAS-RB, Grandstream UCM 6301.

Mikrotik RB2011UiAS-RB	Grandstream UCM 6301.
Enrutamiento dinámico, punto de acceso, cortafuegos, MPLS, VPN, calidad avanzada de servicio, equilibrio de carga y unión, configuración y monitoreo en tiempo real.	Plataforma de conferencias y reuniones incorporada; admite terminales de escritorio, aplicaciones Wave y SIP.
Tecnología de conectividad Ethernet	Protección de seguridad avanzada con arranque seguro, certificado único y contraseña predeterminada aleatoria para proteger llamadas y cuentas
CPU de arquitectura ARM para un rendimiento más alto	Compatible con GDMS para configuración, administración y monitoreo en la nube.
Conexión de red compatible con VPN	Los navegadores Wave para Android, iOS, Chrome y Firefox permiten la comunicación con todos los usuarios

Elaborado por: El Investigador

- **Configuración Router Quisapincha**

En esta etapa se llevan a cabo las configuraciones de los routers Mikrotik RB2011UiAS-RB, los cuales desempeñan un papel fundamental en la implementación del diseño del sistema de comunicación. Para ello, se utiliza la aplicación WinBox para la programación del router Mikrotik RB2011UiAS-RB. En la figura 28 se observa la configuración del router de la sucursal Quisapincha.

Las fotografías del prototipo implementado se encuentran en el Anexo I.

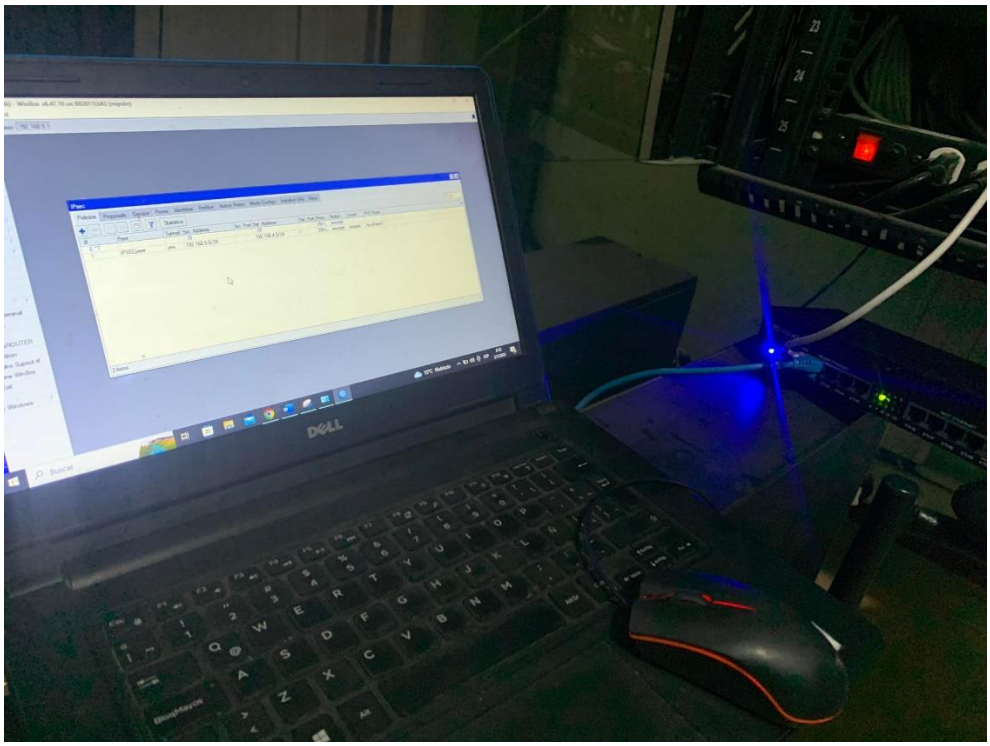


Figura 28. Configuración router Mikrotik RB2011UiAS-RB-Quisapincha

Elaborado por: El Investigador

Se accede al router con el propósito de ajustar los diversos parámetros de conectividad en este caso la clave de contraseña direccionamiento como se muestra en la figura 29.

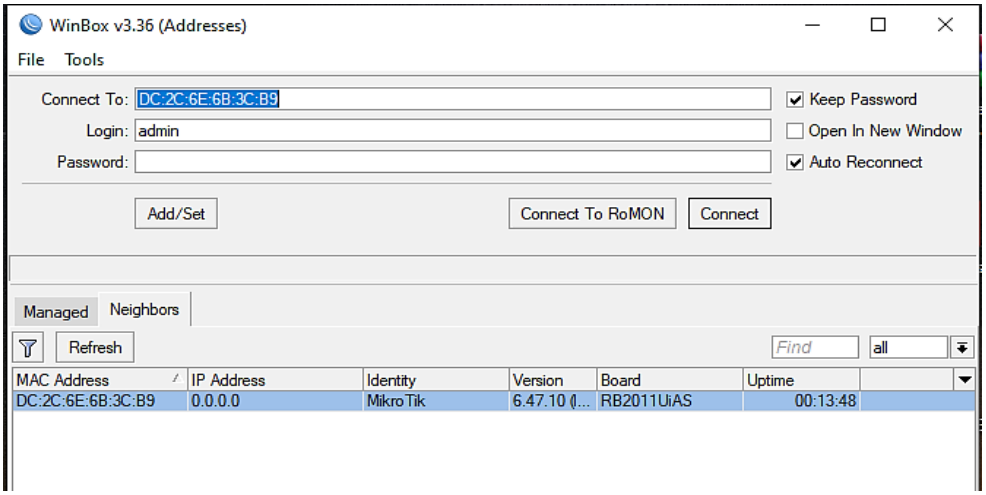


Figura 29. Configuración de router direccionamiento y conectividad

Elaborado por: El Investigador

Se procede a añadir una dirección IP específica al router, la cual se muestra en la figura 30.

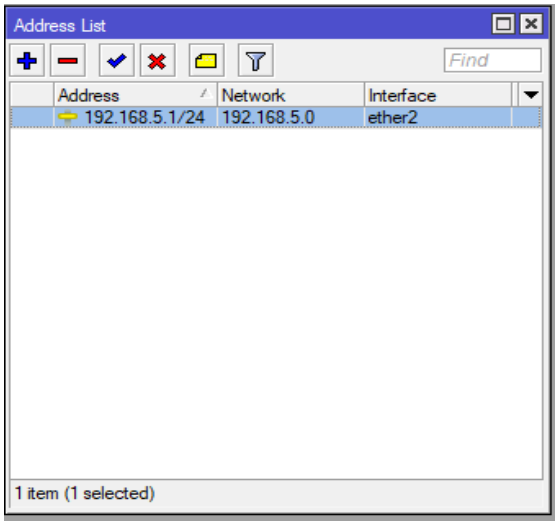


Figura 30. Asignación de dirección IP en el router

Elaborado por: El Investigador

Se continua con el ingreso al Router por medio de la IP y direccionamiento agregado, como se visualiza en la figura 31.

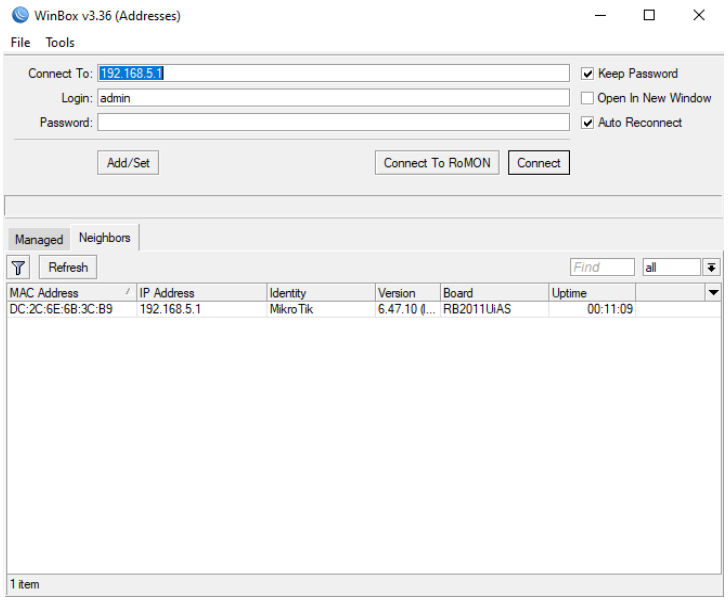


Figura 31. Ingreso al Router

Elaborado por: El Investigador

Al activar el puerto 500, en el protocolo UDP se habilita la transmisión de datos necesaria para permitir la comunicación, asignando un puerto de conectividad específico (en este caso, el puerto 500) y utilizando el protocolo UDP. El proceso se ilustra en la figura 32.

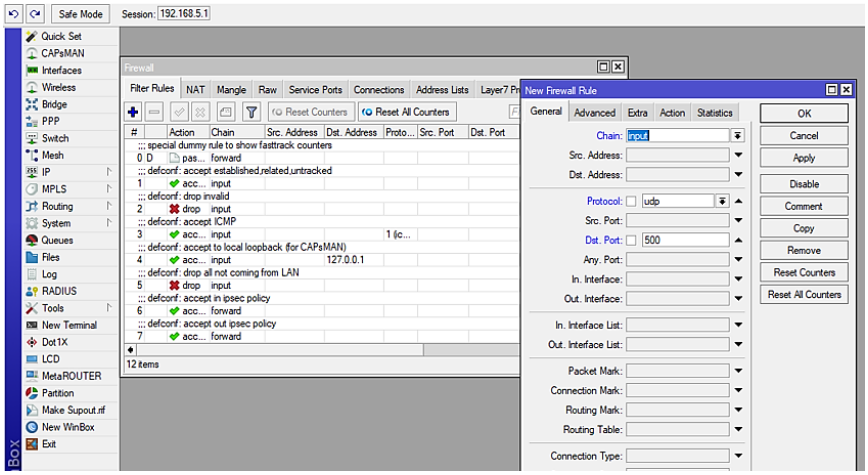


Figura 32. Activación del puerto y protocolo UDP

Elaborado por: El Investigador

En este apartado se establece el sistema de seguridad de red para proteger y autenticar las comunicaciones realizadas a través de IPsec. Esto implica la configuración de parámetros como la encriptación, la autenticación, el cifrado, la asignación de claves y la definición de túneles VPN, todo ello con el objetivo de garantizar la seguridad en las comunicaciones de la red, la figura 33 representa el proceso.

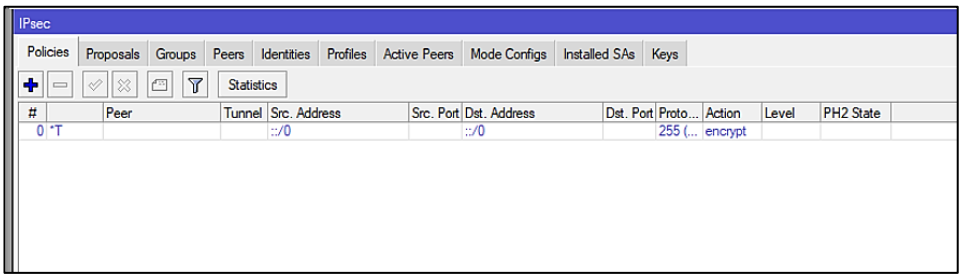


Figura 33. Configuración IPSEC

Elaborado por: El Investigador

Se lleva a cabo la creación de un perfil de seguridad y encriptación con el fin de establecer una configuración específica para el proceso de comunicación y así

garantizar la seguridad de la información que se transmite a través de la red, como se muestra en la figura 34. Esta medida es esencial para asegurar la protección de la información transmitida.

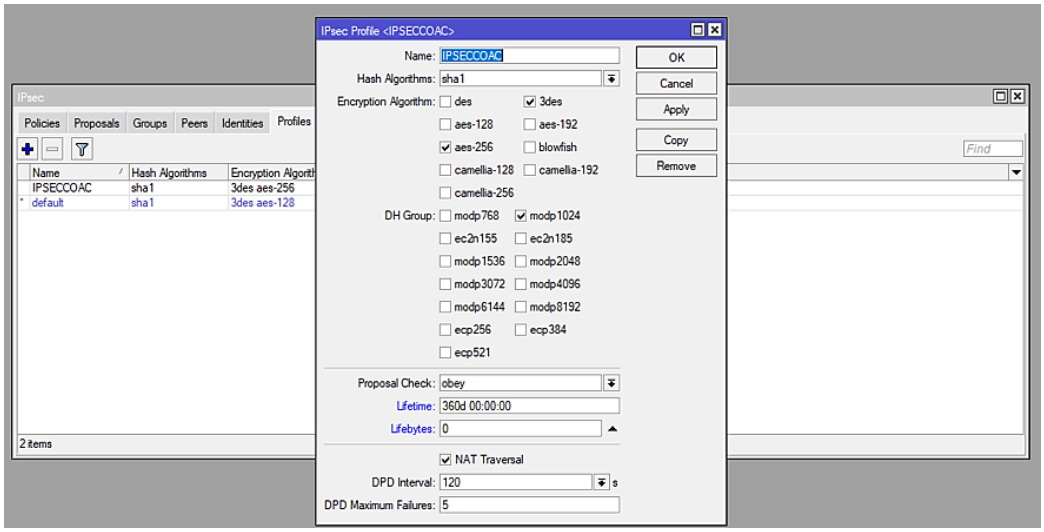


Figura 34. Perfil de seguridad y encriptación

Elaborado por: El Investigador

Se prosigue con la configuración del router ingresando la dirección IP pública de la matriz, junto con el puerto utilizado para la comunicación en la red. Este proceso se ilustra en la figura 35.

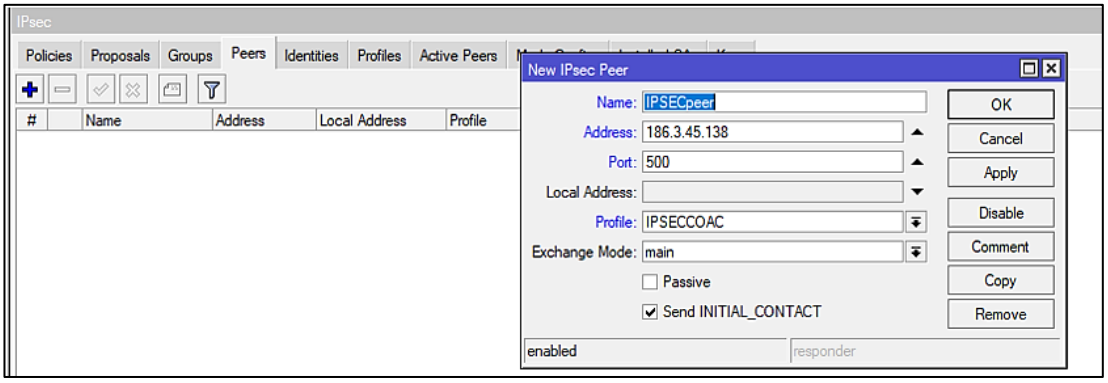


Figura 35. Ingreso a la IP pública y puerto de comunicación de la matriz

Elaborado por: El Investigador

Con el fin de proteger la comunicación y asegurar la privacidad y confidencialidad de la información transmitida en la red, se crea una seguridad, clave o contraseña. Esta

medida de seguridad, se encarga de proteger la información transmitida y garantizar que solo los usuarios autorizados tengan acceso a ella. En la figura 36 correspondiente se puede observar el proceso de creación de la seguridad.

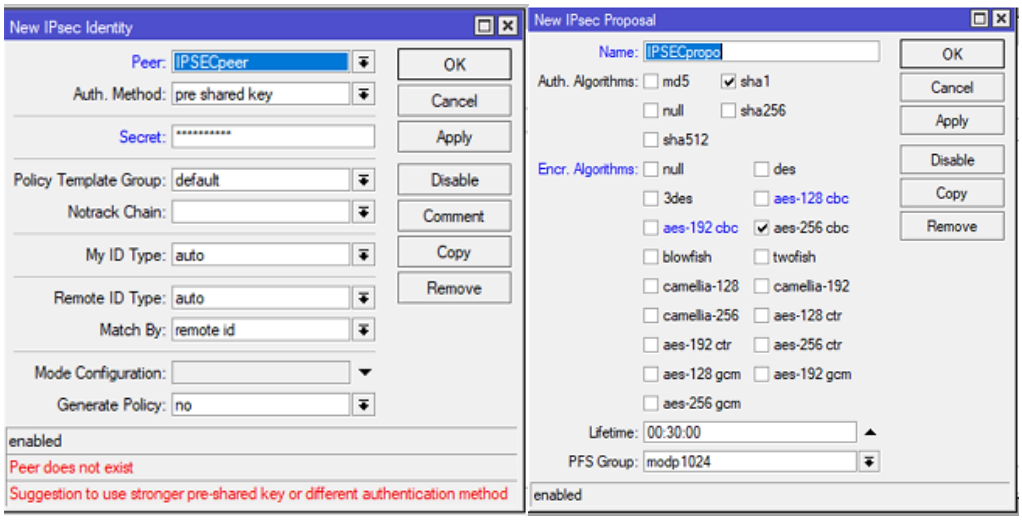


Figura 36. Creación de seguridad para establecer la comunicación

Elaborado por: El Investigador

Luego de haber creado los parámetros de seguridad, se procede a ingresar las direcciones IP correspondientes a la red LAN de la matriz y la sucursal. Este proceso se muestra en la figura 37.

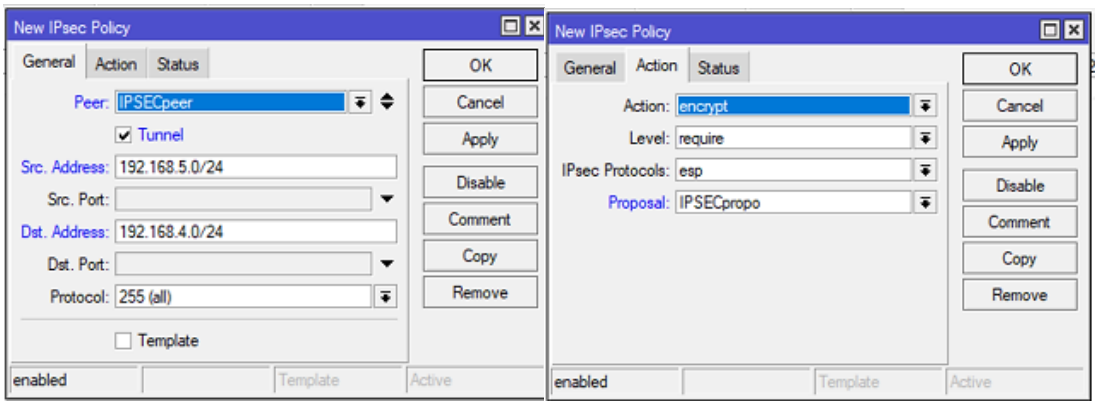


Figura 37. Ingreso a las direcciones IP matriz-sucursal

Elaborado por: El Investigador

Configurado el router de la sucursal de Quisapincha se repite el mismo proceso para el router de la matriz Ambato, ya que como se puede observar en la figura 38, aún no se ha establecido la comunicación.

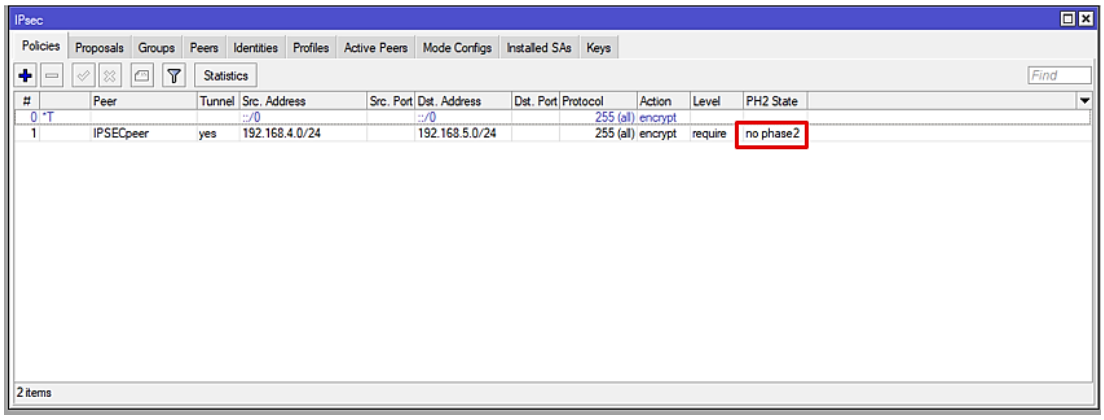


Figura 38. Limitación de comunicación

Elaborado por: El Investigador

- **Configuración Router Matriz Ambato**

Las fotografías del prototipo implementado se encuentran en el Anexo J.

Se procede de la misma manera utilizando la aplicación WinBox con el fin de programar el router Mikrotik. En la figura 39, se observa el dispositivo físico en la matriz Ambato.

Figura 39. Configuración Router Ambato

Elaborado por: El Investigador

Se accede al router para establecer el direccionamiento apropiado como se muestra en la figura 40.

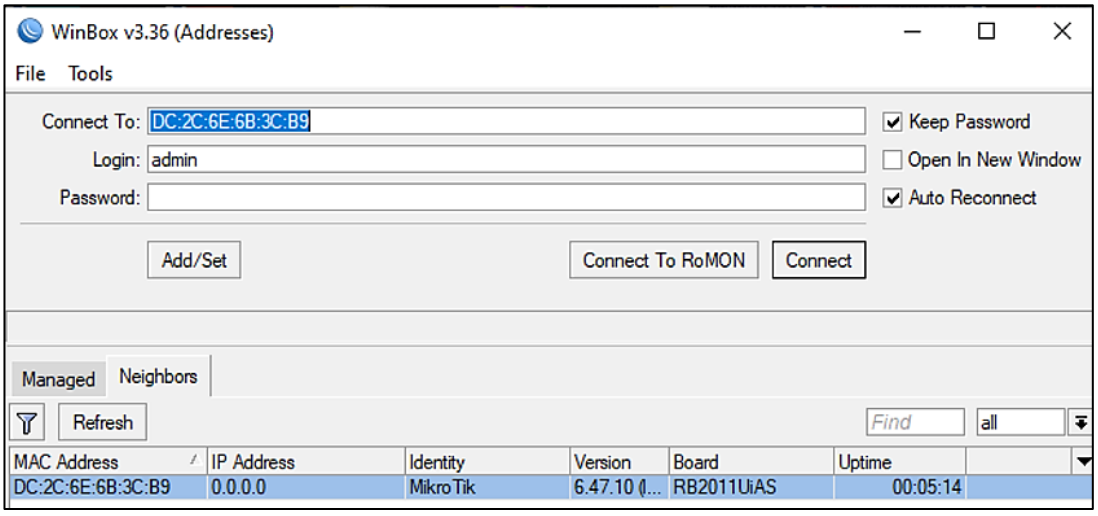


Figura 40. Configuración de router Ambato, direccionamiento y conectividad

Elaborado por: El Investigador

Activación del puerto 500 y el protocolo UDP para habilitar la transmisión de datos, se establecen las mismas condiciones para permitir la comunicación. El proceso se ilustra en la figura 41 correspondiente.

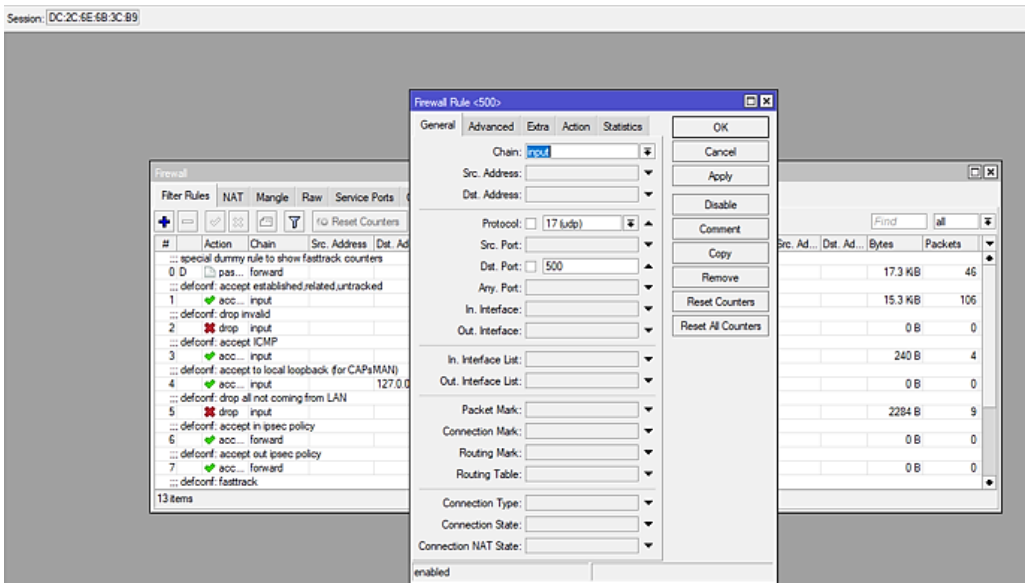


Figura 41. Activación del puerto y protocolo UDP

Elaborado por: El Investigador

De la misma forma se crea un perfil de seguridad y encriptación con el fin de establecer una configuración específica, como se muestra en la figura 42. Esta medida es esencial para asegurar la protección de la información transmitida.

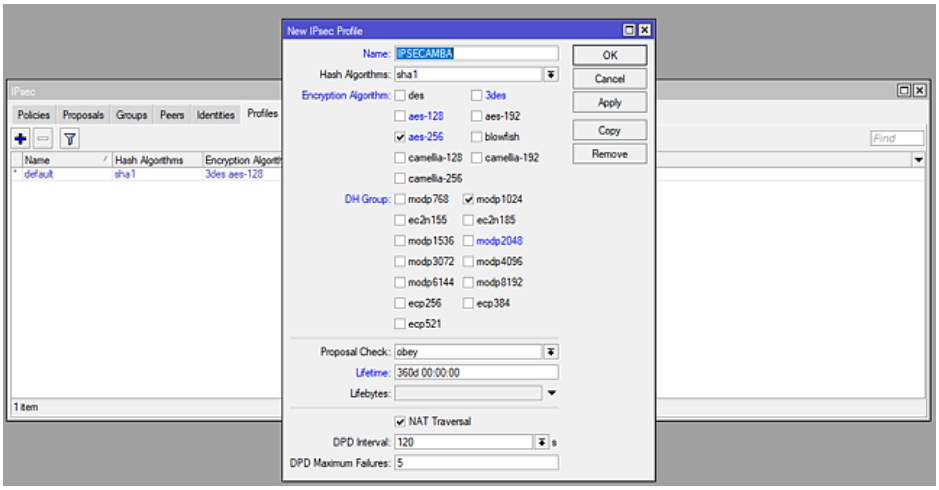


Figura 42. Creación del perfil de seguridad y encriptación

Elaborado por: El Investigador

Se prosigue con la configuración del router ingresando la dirección IP pública de la matriz Ambato, junto con el puerto utilizado para la comunicación en la red. Este proceso se ilustra en la figura 43 correspondiente.

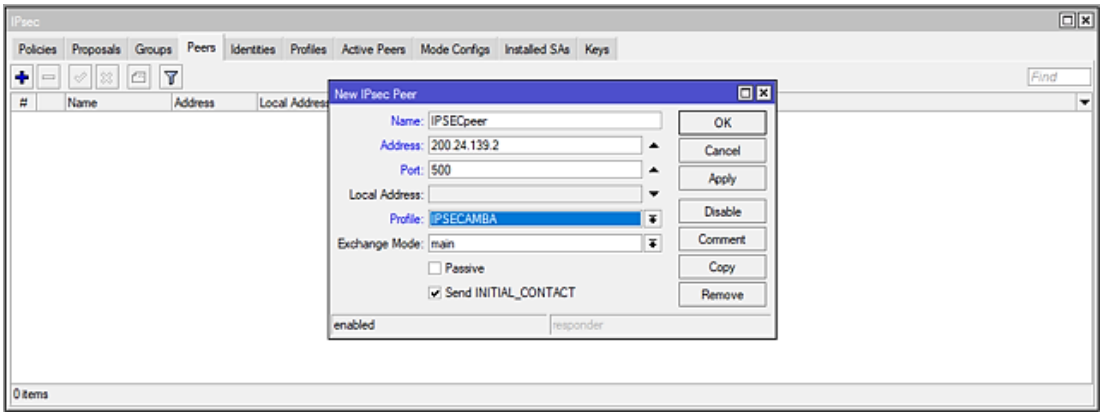


Figura 43. Ingreso a la IP pública y puerto de comunicación de la matriz Ambato

Elaborado por: El Investigador

Al igual que la configuración del router anterior se configura la privacidad y confidencialidad de la información asignando una calve de usuario para tener

autorización de acceso. En la figura 44, se puede observar el proceso de asignación de la clave de seguridad al router mikrotik.

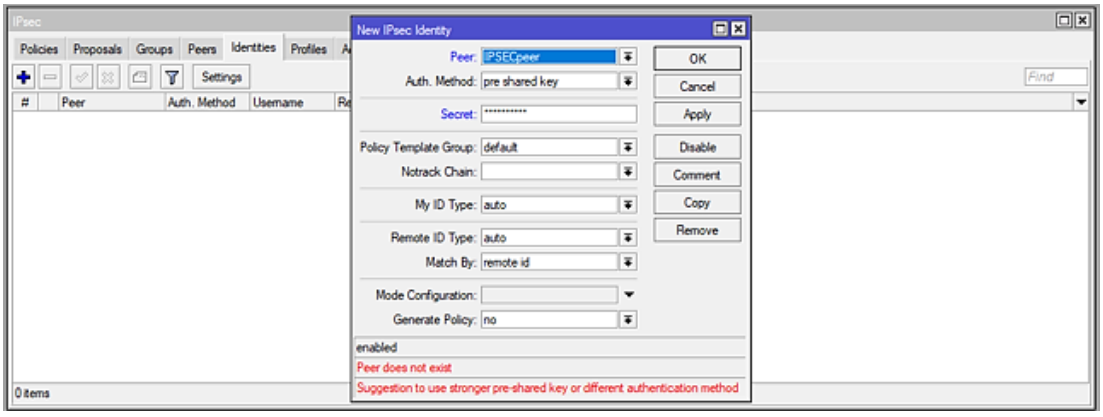


Figura 44. Datos de autorización para establecer la comunicación

Elaborado por: El Investigador

Se procede a ingresar las direcciones IP correspondientes a la LAN de la matriz. Este proceso se muestra en la figura 45.

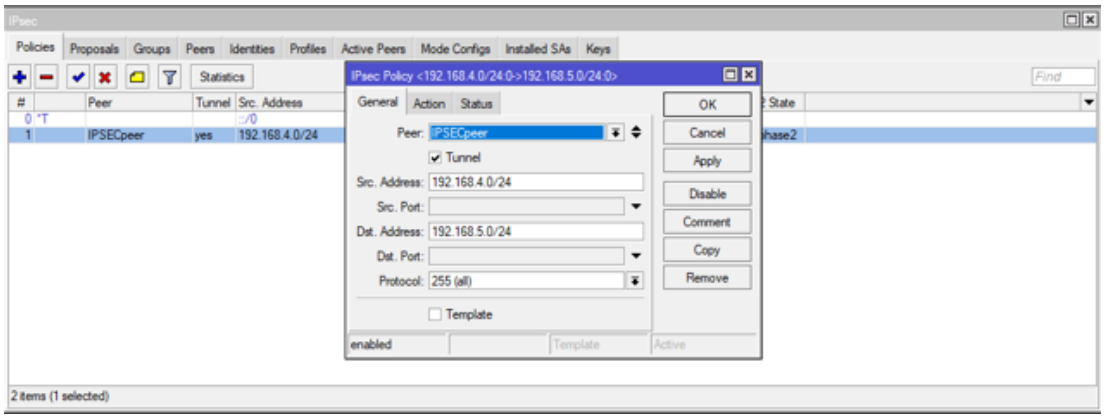


Figura 45. Ingreso a las direcciones IP matriz-Ambato

Elaborado por: El Investigador

Una vez configurados los routers tanto en la sucursal de Quisapincha como en la sucursal de la matriz en Ambato, se procede a verificar si existe comunicación entre ellos y confirmar que el proceso se ha realizado correctamente. En la figura 46, se puede observar que la comunicación ha sido establecida exitosamente.

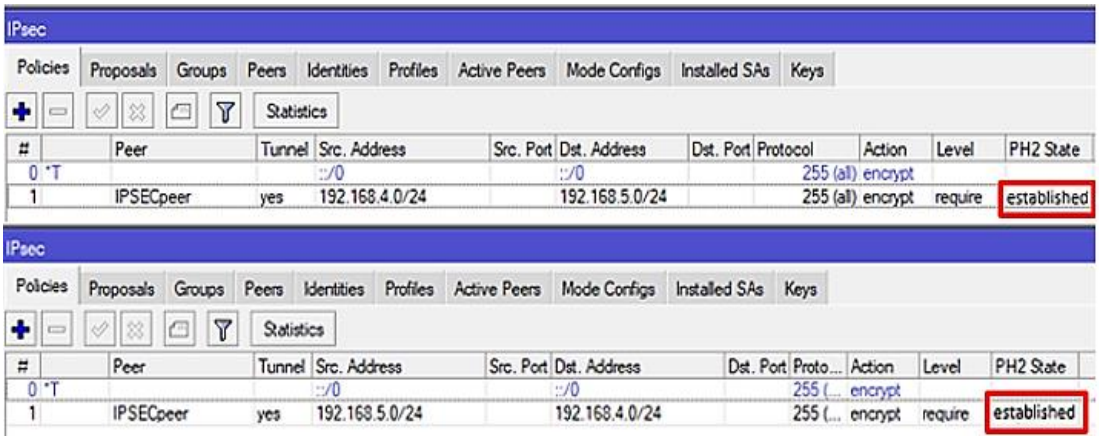


Figura 46. Limitación de comunicación

Elaborado por: El Investigador

- **Configuración de la NAT**

La configuración de NAT es un procedimiento fundamental para conectar dispositivos en diferentes sucursales y permitir la comunicación entre ellos, a la vez que brinda seguridad en redes privadas y públicas.

Se configuran las direcciones IP públicas y privadas que son proporcionadas por el proveedor, junto con la dirección interna de la red, con el fin de establecer NAT y permitir la comunicación entre los dispositivos, como se observa en la figura 47.

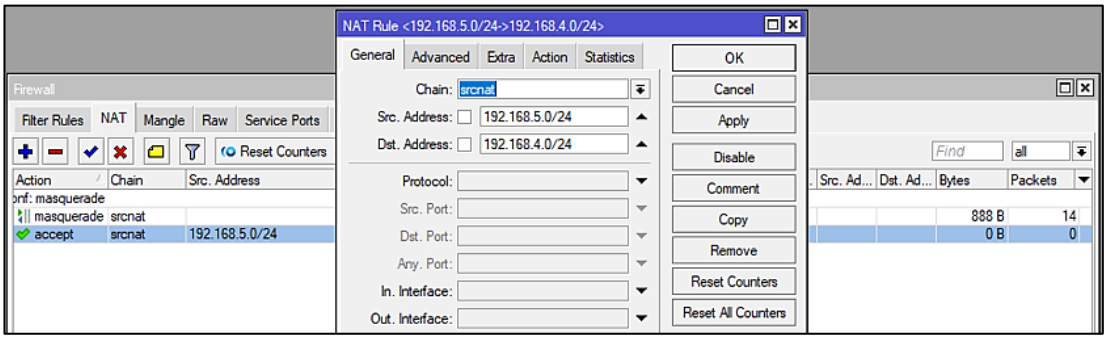


Figura 47. Configuración de las direcciones IP publicas y privadas

Elaborado por: El Investigador

Después de configurar las direcciones IP, se lleva a cabo un reinicio para asegurar que los cambios se hayan guardado exitosamente. Como se muestra en la figura 48.

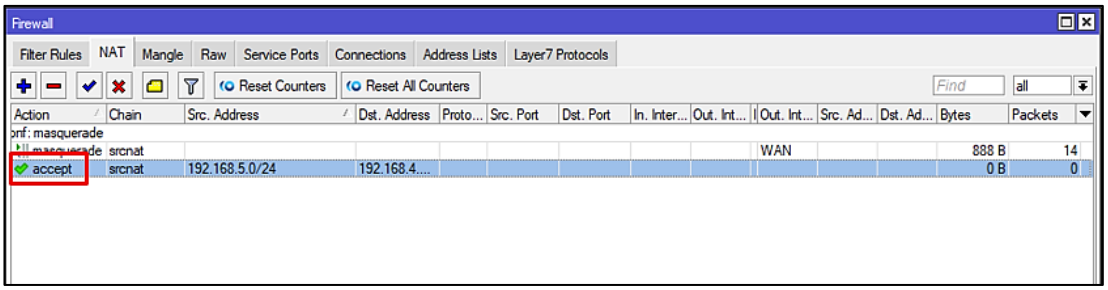


Figura 48. Comprobación del funcionamiento correcto de la NAT

Elaborado por: El Investigador

Configuración sala de monitoreo

En la sala de monitoreo se procede a la configuración del DVR, tanto en la sucursal Quisapincha como en la matriz Ambato. La implementación de un monitor y fotografías del prototipo implementado se encuentran en el Anexo K.

- **Configuración DVR Quisapincha**

La configuración del DVR resulta crucial con el fin de permitir la modificación de los parámetros de seguridad y almacenamiento de datos, los ajustes adaptados para un sistema específico de video vigilancia. Con este propósito, se procede a la identificación de la dirección IP del DVR, mediante la utilización del programa SADPTool. En la figura 49 se visualiza la configuración.

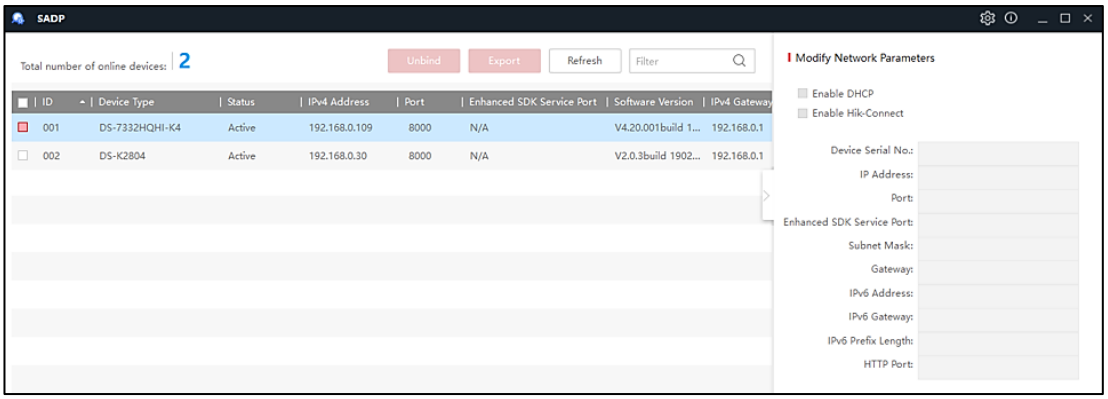


Figura 49. Localización de la IP del DVR

Elaborado por: El Investigador

Una vez identificado la IP se direcciona a la interfaz principal como se muestra en la figura 50.

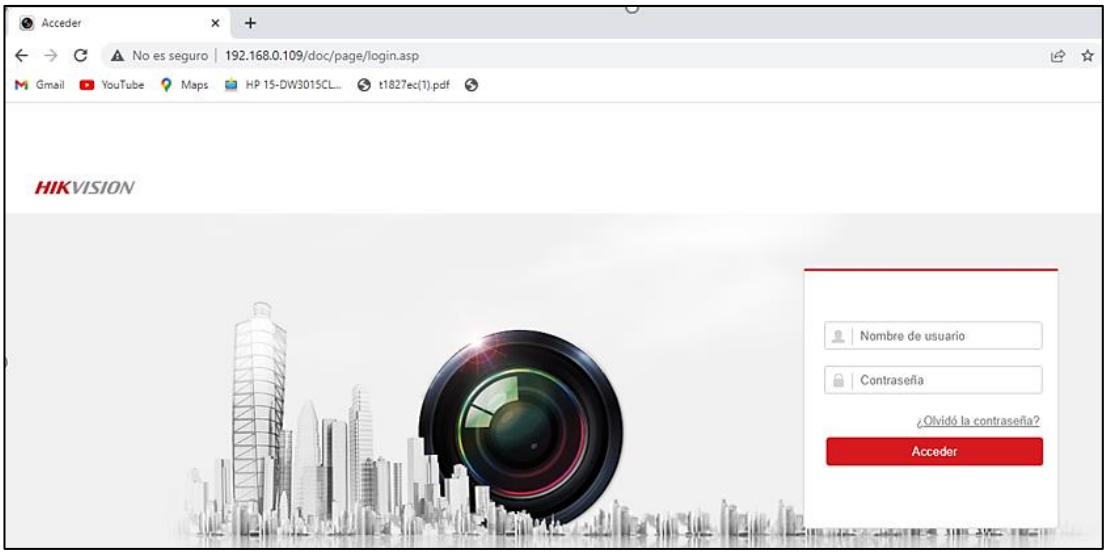


Figura 50. Direccionamiento a la interfaz principal

Elaborado por: El Investigador

Para ingresar al sistema de video vigilancia se lo realiza con la autenticación del nombre de usuario y la contraseña, en la figura 51 se muestra el ingreso al sistema de seguridad en tiempo real.

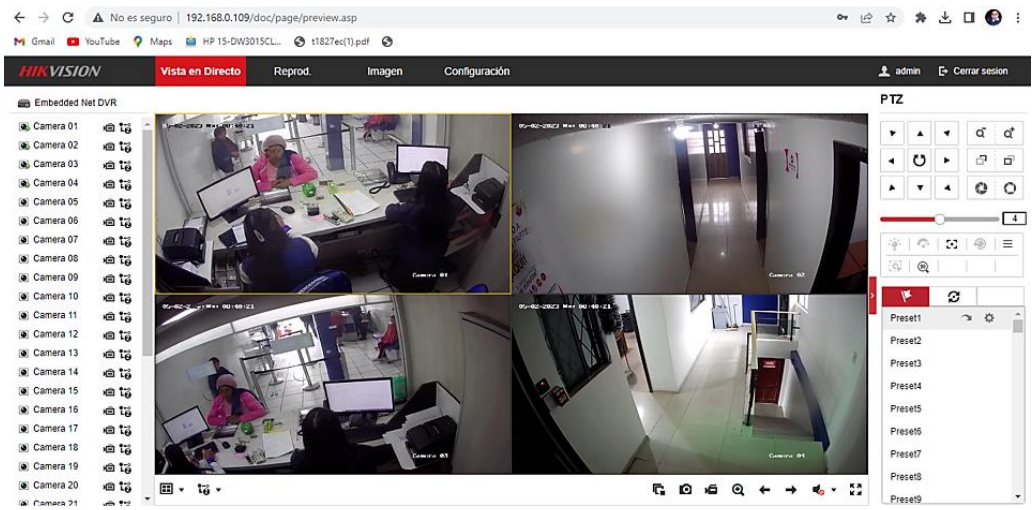


Figura 51. Ingreso al sistema de seguridad en vista en directo

Elaborado por: El Investigador

Posteriormente, se procede a ingresar la nueva dirección IP con el fin de configurar los ajustes básicos del sistema, de acuerdo con los parámetros de calidad de imagen y resolución de video previamente establecidos, tal como se muestra en la figura 52.

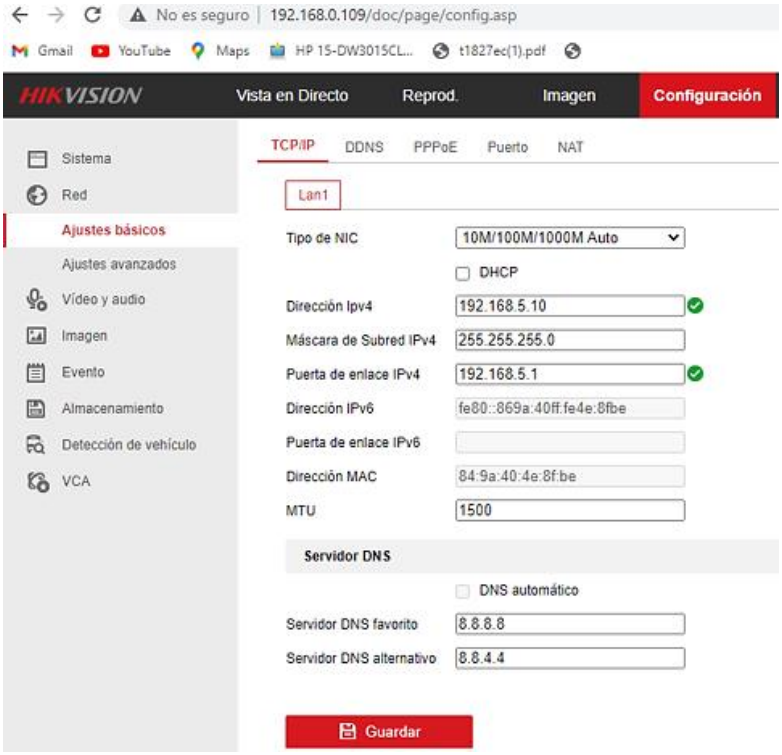


Figura 52. Configuracion de IP del sistema

Elaborado por: El Investigador

En la figura 52, se observan las cámaras de la matriz Ambato y sucursal Quisapincha de la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua que son necesarios para la creación de la sala de monitoreo de video vigilancia.

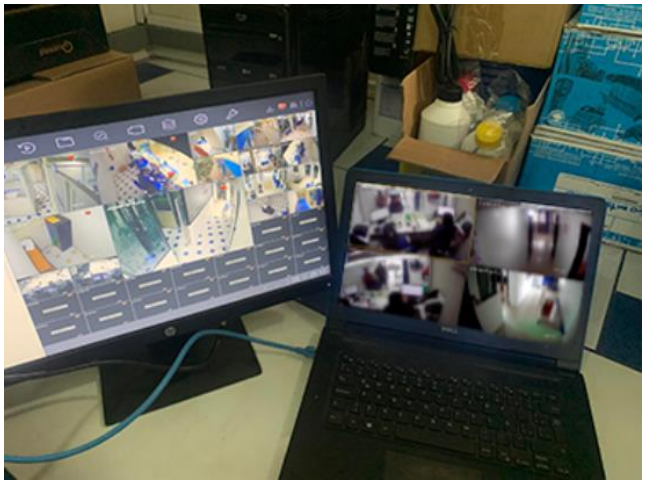


Figura 53. Acceso a las cámaras de la matriz y sucursal Quisapincha

Elaborado por: El Investigador

3.2.4 Configuración de la central telefónica

El equipo Grandstream UCM6301 facilita la configuración de la central telefónica mediante su interfaz intuitiva. Para lograrlo, se accedió a la dirección IP local y se configuraron aspectos como las líneas troncales, extensiones y enrutamiento de llamadas. Además, se estableció la conexión de los dispositivos de telefonía IP con la central, lo que permitió realizar y recibir video llamadas de alta calidad. Con base en estos parámetros, se ajustó la configuración de la sala de videoconferencias para proporcionar un rendimiento óptimo, como se muestra en la figura 54. Las fotografías de la implementación de la central UCM6301 se observa en el Anexo L.

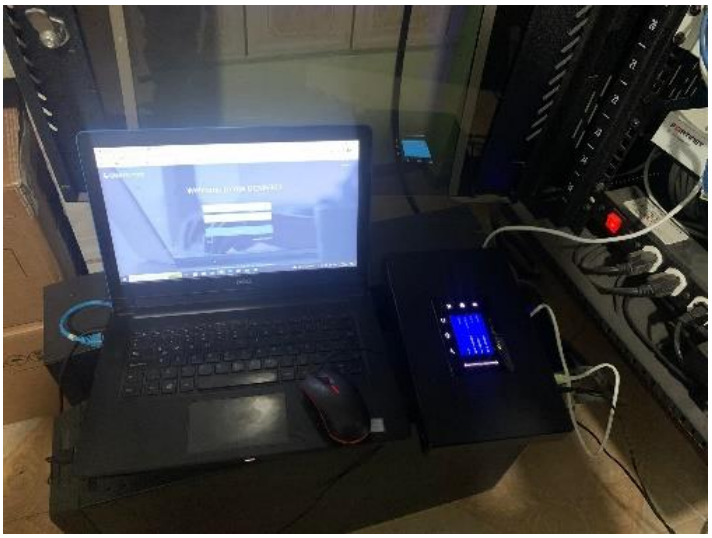


Figura 54. Configuración de la central utilizando Grandstream UCM6301

Elaborado por: El Investigador

Una vez familiarizado sobre los pasos a tomar en cuenta, se procede a acceder al panel de configuración de GRANDSTREAM para elegir la herramienta Wave, que posibilita la configuración de la sala de conferencias. En la figura 55, se observa el acceso a la interfaz correspondiente.

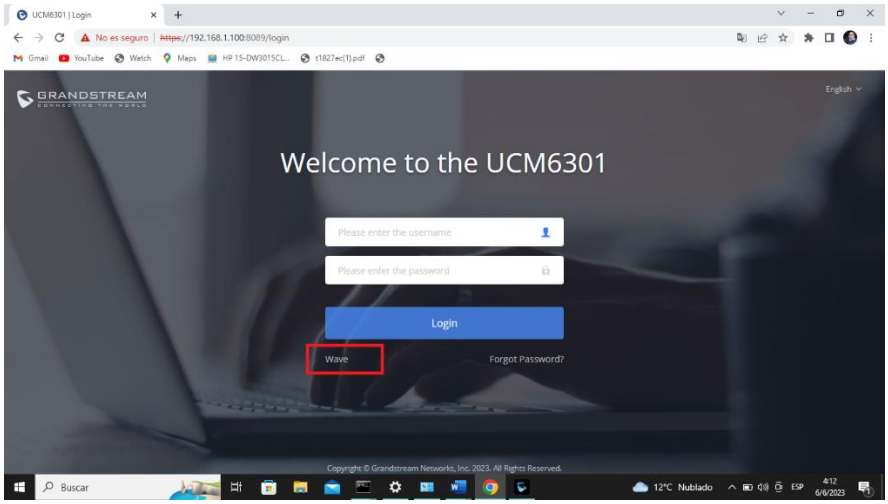


Figura 55. Ingreso al panel de configuración de GRANDSTREAM

Elaborado por: El Investigador

Antes de proceder con la configuración de la central telefónica IP, se verifica la conectividad de la red para garantizar un acceso sin problemas a la interfaz de administración. Durante este proceso, se configuran los parámetros de red y el dominio correspondiente, así como las extensiones básicas necesarias. La figura 56, ilustra el proceso de configuración de la IP de la central telefónica.

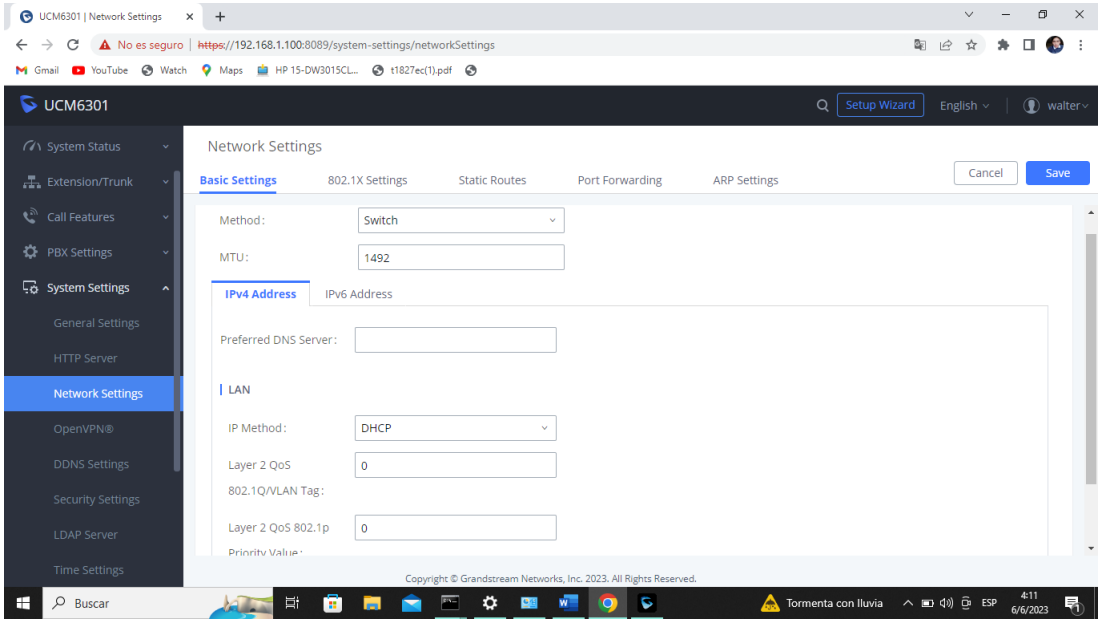


Figura 56. Configuración IP central telefónica

Elaborado por: El Investigador

Para configurar una dirección IP estática, se procede a acceder a la interfaz de administración del dispositivo que está conectado a la misma red que la central telefónica. A través de la interfaz web, se utiliza la dirección IP para ingresar a la interfaz de administración y se navega hasta la sección de configuración de red. Allí se selecciona la opción de configuración de IP estática y se ingresan los parámetros específicos para establecer una conectividad adecuada. Una vez realizados los cambios, se guardan y se reinicia el dispositivo para que los cambios surtan efecto. La figura 57 muestra la interfaz de configuración de la dirección IP estática.

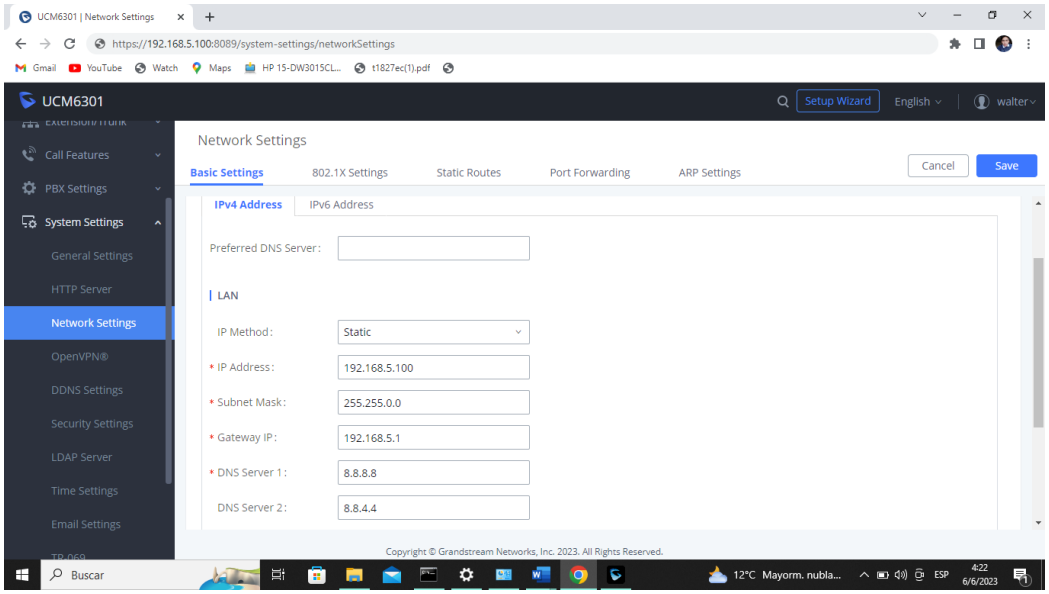


Figura 57. Configuración de la IP estática.

Elaborado por: El Investigador

Una vez que se ha configurado correctamente la dirección IP estática, se verifica que la central telefónica esté conectada a la red ingresando la siguiente dirección en la barra de direcciones: **"http://192.168.5.100".** Este proceso se ilustra en la figura 58.

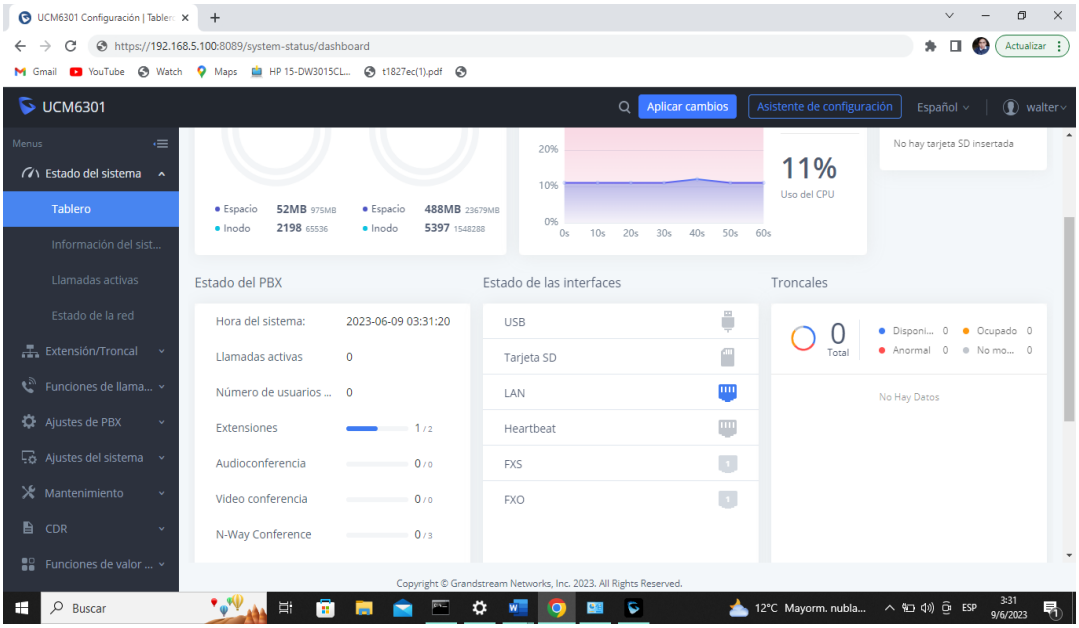


Figura 58. Configuración de la central UCM6301 con la nueva dirección IP.

Elaborado por: El Investigador

A continuación, se crear las extensiones para la matriz de Ambato y la sucursal de Quisapincha, detalladas de la siguiente manera:

Extensión 1000: Gerencia Ambato

Extensión 1001: Agencia Quisapincha

Para la creación de estas extensiones, se deben configurar varios parámetros, como la contraseña, la preferencia de mensajes de voz, y el nombre del departamento o persona asignada al teléfono para identificar la extensión utilizada en la central telefónica. La figura 59, muestra el proceso de creación y configuración de estas extensiones.

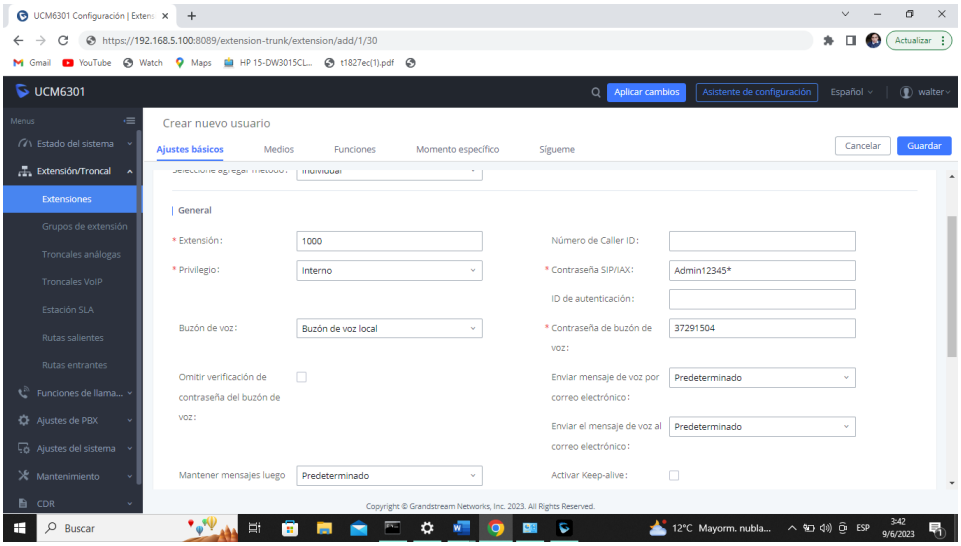


Figura 59. Creación de extensiones para la matriz Ambato y la sucursal de Quisapincha

Elaborado por: El Investigador

Una vez que se hayan creado las extensiones, en la figura 60 se muestra que no están disponibles. Esto se debe a que las extensiones deben registrarse en los dispositivos terminales correspondientes para poder realizar y recibir llamadas de manera adecuada. Para lograrlo es necesario registrar los dispositivos terminales con su respectiva extensión.

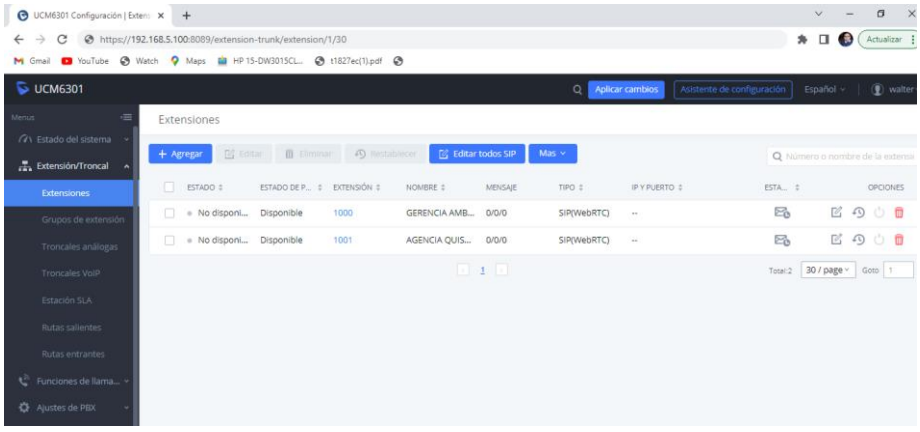


Figura 60. Registro y activación de extensiones

Elaborado por: El Investigador

Para el cliente o equipo terminal, se utiliza la aplicación Wave debido a que la Cooperativa de Ahorro y Crédito Vencedores, actualmente no cuenta con teléfonos IP

compatibles con video llamadas. Esta aplicación proporciona la capacidad de realizar llamadas de voz, video llamadas, y otras funciones relacionadas. Esto se muestra en la figura 61 correspondiente.

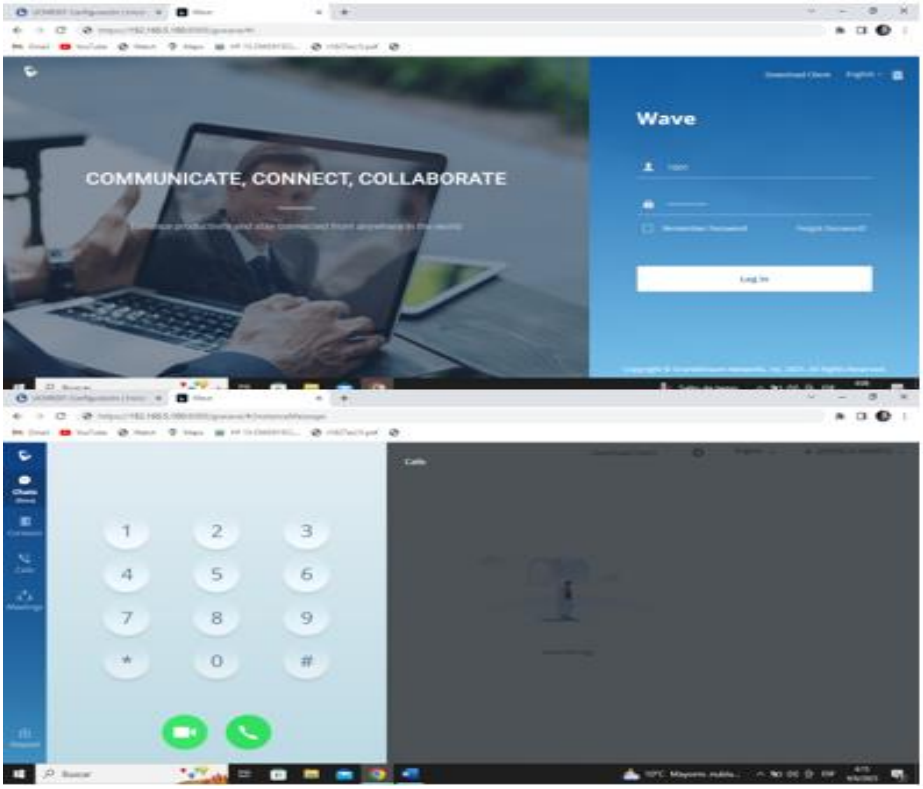


Figura 61. Ingreso a la aplicación Wave

Elaborado por: El Investigador

Como se puede ver en la figura 62, al ingresar al wave en la central UCM se muestran las extensiones creadas y configuradas con anterioridad. La prueba de funcionamiento entre la matriz y sucursal Quisapincha se puede observar en el Anexo M.

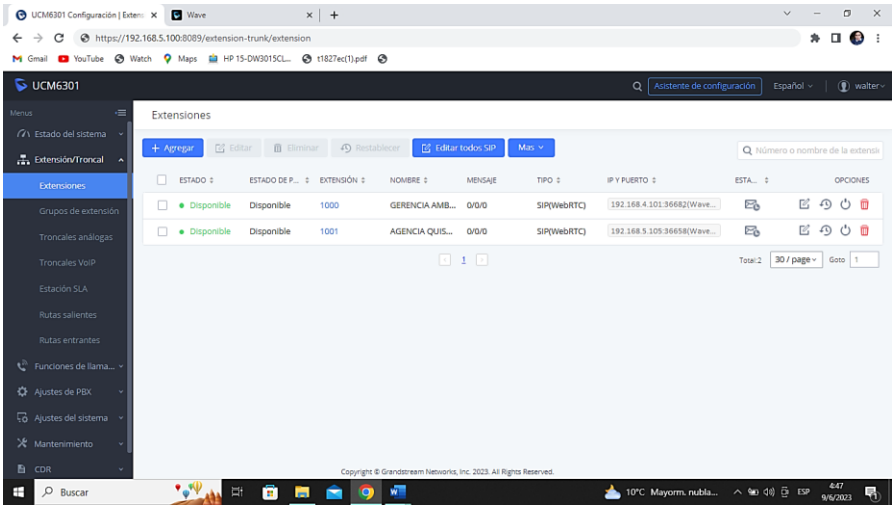


Figura 62. Extensiones creadas y configuradas

Elaborado por: El Investigador

La herramienta GRANSTREM proporciona un servicio denominado GDMS Cloud, el cual permite la gestión y supervisión de dispositivos de telefonía IP y cámaras de seguridad. Para activar dicho servicio, solo se necesita crear una cuenta que brinda acceso a las funciones de control y administración de los dispositivos a través de una interfaz única. En la figura adjunta se presenta la interfaz del GDMS.

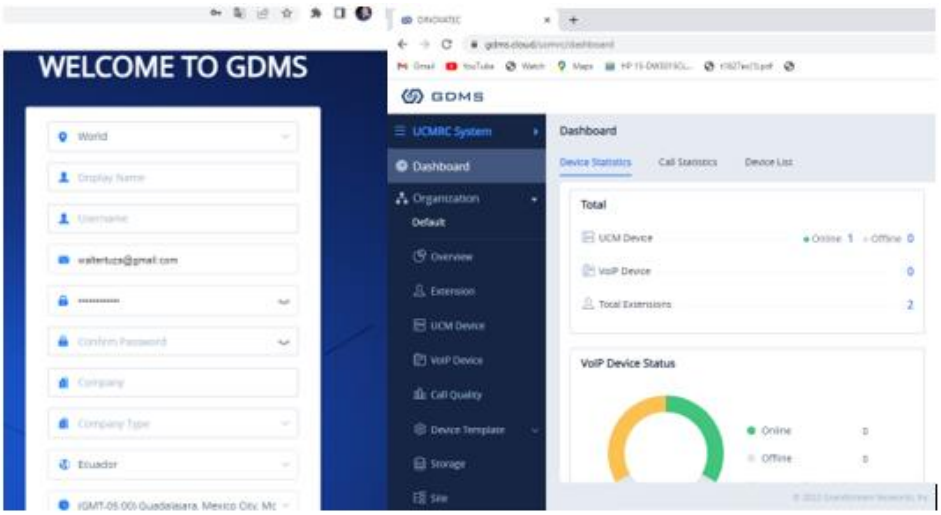


Figura 63. Creación de cuenta GDMS Cloud

Elaborado por: El Investigador

Después de haber creado la cuenta, el siguiente paso es iniciar sesión y transferir la configuración de la central UCM6301 a la nube. Para llevar a cabo esta tarea, resulta

fundamental tener presente la dirección MAC y la contraseña proporcionadas en el dispositivo, como se muestra en la figura adjunta.

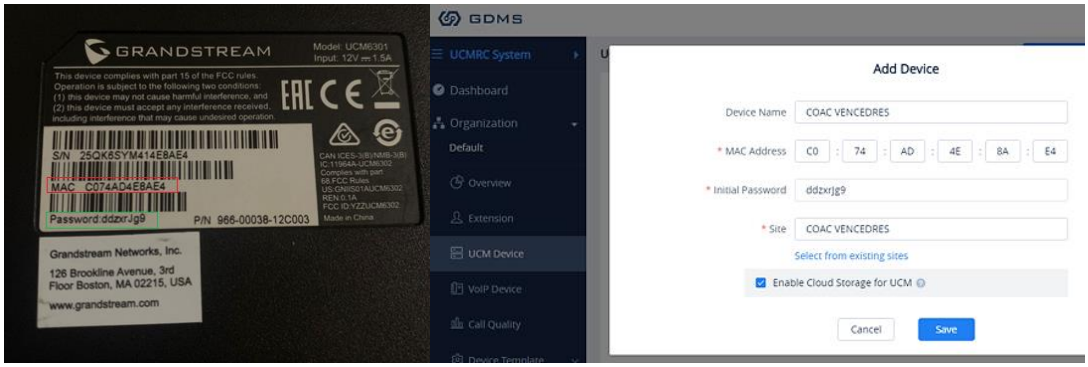


Figura 64. Acceso y subida de la central telefónica a la nube

Elaborado por: El Investigador

Una vez que se han ingresado correctamente los datos, la central UCM6301 creada se activa, como se muestra en la figura 65 adjunta. Esto permite obtener acceso remoto al UMC, lo que resulta beneficioso para conectar con clientes ubicados en diferentes lugares, no limitándose únicamente a la oficina.

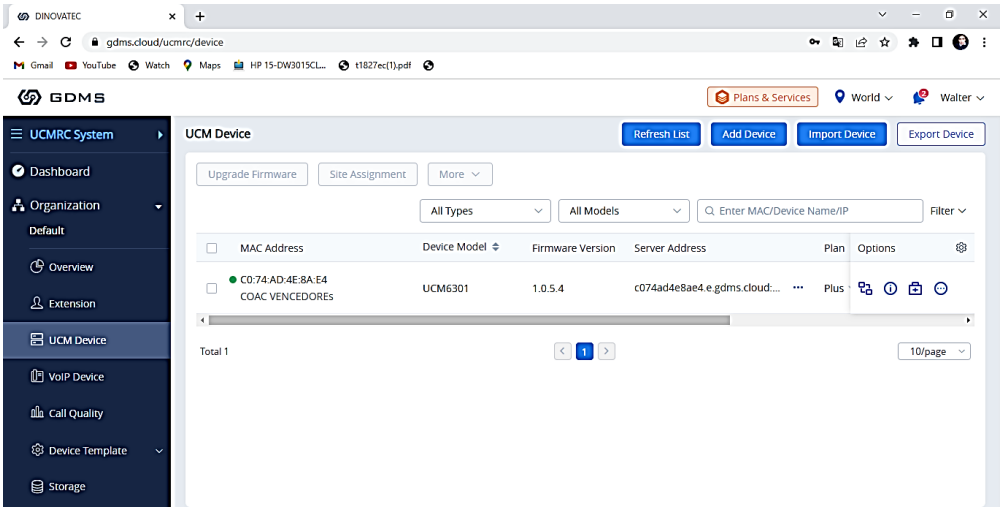


Figura 65. Activación de la central creada UCM6301

Elaborado por: El Investigador

Posteriormente, es necesario proceder a descargar el cliente Wave e instalarlo en la computadora. Una vez instalado, se solicita ingresar el servidor al cual se desea

conectar, así como la extensión y su respectiva contraseña como se muestra en la figura 66.

Figura 66. Configuración e instalación del cliente wave e en la PC.

Elaborado por: El Investigador

El servidor al cual se accedió, ofrece la misma plataforma por lo cual se copia el mismo enlace como se muestra en la figura 67.

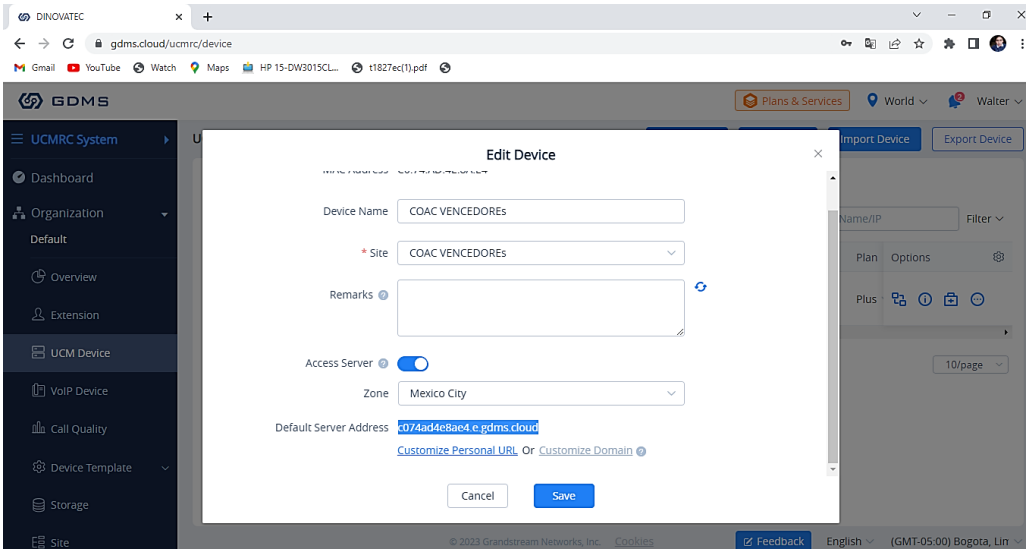


Figura 67. Acceso del servidor

Elaborado por: El Investigador

Finalmente, en la interfaz wave se llena todos los campos previamente configurados en la interfaz UMC6301, como se puede observar en la figura 68, ingresamos la extensión y contraseña antes establecida.

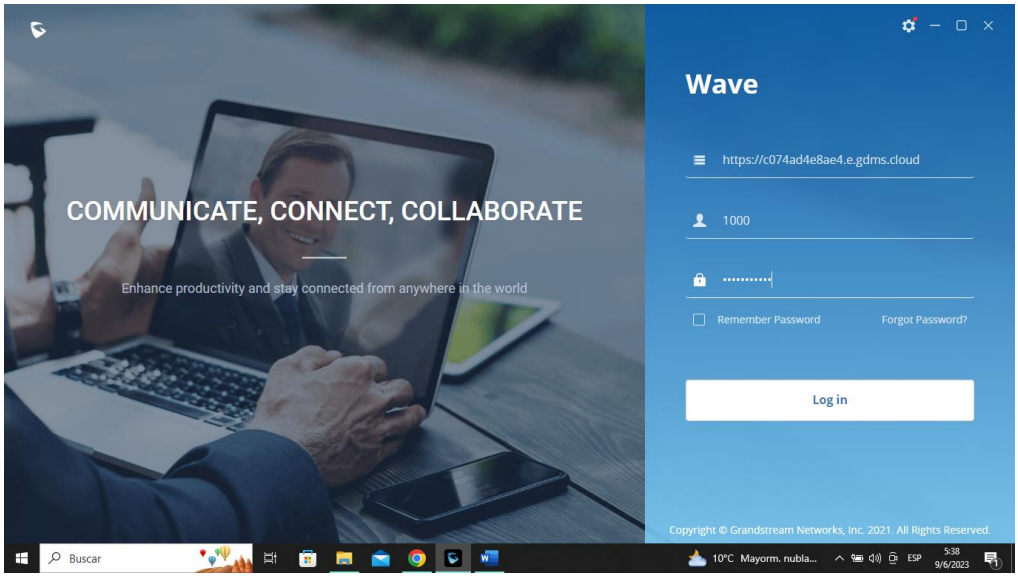


Figura 68. Llenado de campos del servidor

Elaborado por: El Investigador

En este apartado ingresando a la aplicación wave se da los permisos de cámara y video, con el fin de tener llamadas, videos llamadas y sala de video conferencia como se visualiza en la figura 69.

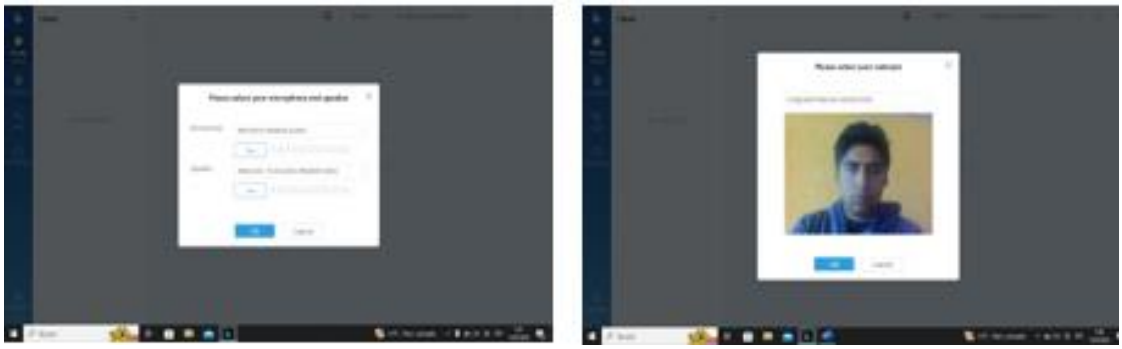


Figura 69. Activación de permisos de cámara y video

Elaborado por: El Investigador

3.2.5 Cálculo de ancho de banda

Para realizar el cálculo de ancho de banda primero es esencial detectar los potenciales puntos de congestión en el sistema de comunicación, incluso si se cuenta con una amplia capacidad de ancho de banda en el enlace WAN o conexión a Internet. La presencia de cuellos de botella internos en la red puede tener un impacto significativo

en su rendimiento y eficiencia. No importa cuán alta sea la capacidad de transmisión externa, si existen limitaciones internas, se pueden producir interrupciones y una reducción general en la calidad del servicio. Por lo tanto, resulta fundamental identificar y resolver cualquier posible obstrucción dentro de la red para garantizar un flujo óptimo de datos y una experiencia fluida para los usuarios, en la figura 70 se demuestra estos "cuellos de botella" y los dispositivos utilizados en el proyecto con la velocidad de transferencia de datos en la red.

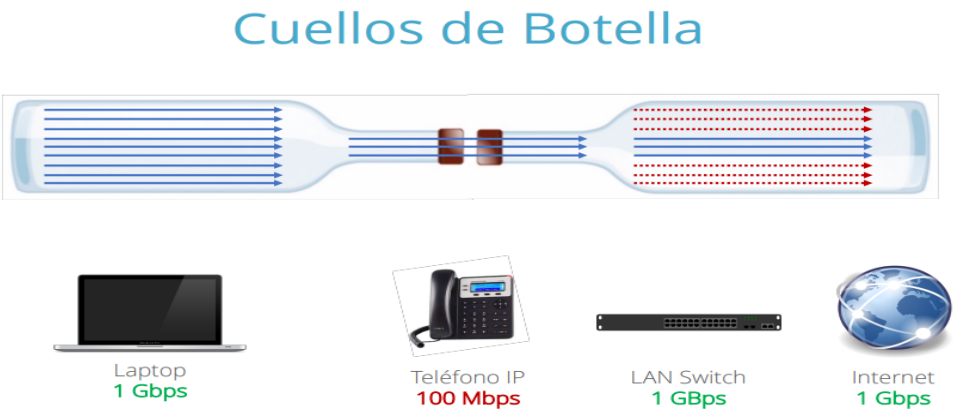


Figura 70. Cuellos de botella internos en la red

Elaborado por: El Investigador

La siguiente etapa consiste en reconocer y conocer los dispositivos presentes en la red, recopilando datos técnicos de cada uno de ellos. Un ejemplo ilustrativo se presenta en la figura 71, donde se muestra el tipo de dispositivos y sus velocidades de transmisión en la red.

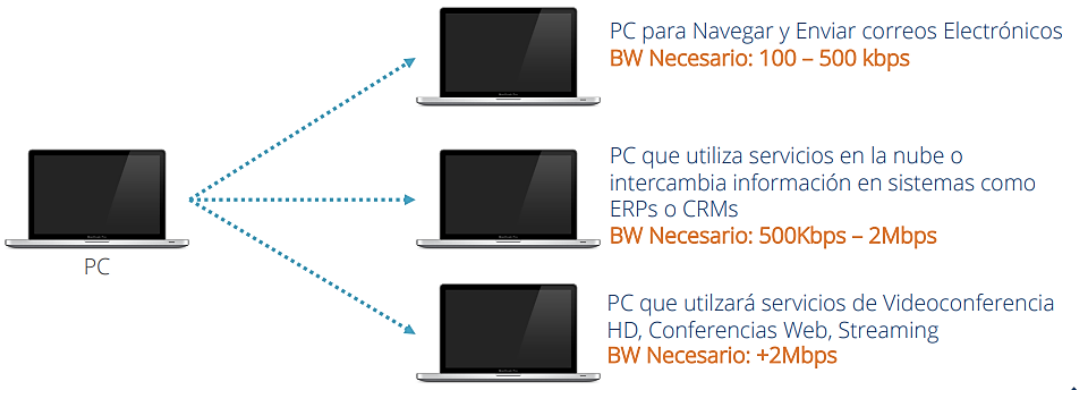


Figura 71. Tipo de dispositivos dentro de la red

Elaborado por: El Investigador

También se identifican los dispositivos de bajo consumo. En la figura 72 se muestran algunos de estos dispositivos que tienen poco consumo de ancho de banda.

Figura 72. Dispositivos de bajo consumo

Elaborado por: El Investigador

Identificación de dispositivos de consumo medio. En la figura 73, se muestran algunos ejemplos

Figura 73. Dispositivos de consumo medio

Elaborado por: El Investigador

Identificación de dispositivos de consumo alto. En la figura 74 se muestran estos ejemplos

Figura 74. Dispositivos de consumo alto

Elaborado por: El Investigador

Identificación de dispositivos de intenso consumo. En la figura 75 se muestran estos ejemplos.

Figura 75. Dispositivos de intenso consumo

Elaborado por: El Investigador

Una vez que se hayan identificado los dispositivos, el siguiente paso consiste en calcular el ancho de banda necesario durante una "hora pico" para garantizar que todos los dispositivos dentro de la red puedan funcionar de manera simultánea sin experimentar problemas de rendimiento o congestión.

Este cálculo implica evaluar la cantidad de datos que cada dispositivo puede generar o consumir durante ese periodo de mayor actividad, y sumar estos requisitos de ancho de banda para obtener un valor total. Por lo cual, se aplica la fórmula (1) para el cálculo del ancho de banda.

$$ANCHO\ BANDA = USUARIOS * \ CALIDAD\ DE\ SERVICIO \quad (1)$$

EQUIPOS MATRIZ AMBATO

Dispositivos de bajo consumo

- 12 Teléfonos VoIP Básicos
- 10 Dispositivos computadores que navegan ligeramente

$$ANCHO\ BANDA = 12 * 100Kbps$$

$$ANCHO\ BANDA = 1200\ Kbps$$

$$ANCHO\ BANDA = 1{,}2Mbps$$

Dispositivos de Consumo Medio.

- 8 Computadoras navegando, enviando correos y descargando archivos activamente

$$ANCHO\ BANDA = 8 * \ 250\ Kbps$$

$$ANCHO\ BANDA = 2000\ Kbps$$

$$ANCHO\ BANDA = 2\ Mbps$$

Dispositivos de Consumo Alto

- 2 Computadoras con videoconferencia SD o Conferencias Web

$$ANCHO\ BANDA = 2 * \ 1{,}5\ Mbps$$

$$ANCHO\ BANDA = 3\ \ Mbps$$

Dispositivos de intenso consumo

- 1 Un dispositivo de videoconferencia con una sesión en HD
- DVR HIKVISION.

$$ANCHO\ BANDA = 2 * \ 2{,}5\ Mbps$$

$$ANCHO\ BANDA = 5\ Mbps$$

$$Total\ AB = Dispositivo\ bajo\ consumo + \text{Dispositivos de Consumo Medio} + \text{Dispositivos de Consumo Alto} + \text{Intenso}$$

$$Total\ AB = 1{,}2\ Mbps + 2\ Mbps + 3\ \ Mbps + 5\ Mbps$$

$$Total\ AB = 11{,}2\ Mbps$$

En la figura 76 se observa la velocidad de descarga y subida de transmision de datos, (velocidad de internet).

Figura 76. Velocidad de descarga y subida

Elaborado por: El Investigador

EQUIPOS QUISAPINCHA.

Dispositivo bajo consumo

- 8 Teléfonos VoIP Básicos.
- 11 Dispositivos computadores que navegan ligeramente

$$ANCHO\ BANDA = 19 * 100\ Kbps$$

$$ANCHO\ BANDA = 1900\ Kbps$$

$$ANCHO\ BANDA = 1{,}9\ Mbps$$

Dispositivos de Consumo Medio.

- 5 Computadoras navegando, enviando correos y descargando archivos activamente.

$$ANCHO\ BANDA = 5 * 250\ Kbps$$

$$ANCHO\ BANDA = 1250\ Kbps$$

$$ANCHO\ BANDA = 1{,}3\ Mbps$$

Dispositivos de Consumo Alto

- 1 Computadora con videoconferencia SD o Conferencias Web

$$ANCHO\ BANDA = 1 * 1{,}5\ Mbps$$

$$ANCHO\ BANDA = 1{,}5\ Mbps$$

Dispositivos de consumo intenso

- 1 Un dispositivo de videoconferencia con una sesión en HD
- 1 DVR HIKVISION.
- 2 Servidores de la Cooperativa.

$$ANCHO\ BANDA = 4 * 2{,}5\ Mbps$$

$$ANCHO\ BANDA = 10\ Mbps$$

$$Total\ AB = Dispositivo\ bajo\ consumo + \text{Dispositivos de Consumo Medio} + \text{Dispositivos de Consumo Alto} + \text{Intenso}$$

$$Total\ AB = 1{,}9\ Mbps + 1{,}3\ Mbps + 1{,}5\ Mbps + 10\ Mbps$$

$$Total\ AB = 14{,}7\ Mbps$$

De acuerdo con los cálculos realizados, es evidente que se requiere un ancho de banda mínimo de 14,7 Mbps para asegurar el funcionamiento adecuado de nuestro sistema, como se observa en la figura 77.

Figura 77. Valores de velocidad en Ancho de Banda minimo

Elaborado por: El Investigador

Se puede verificar en la figura 78, que el sistema implementado funciona correctamente

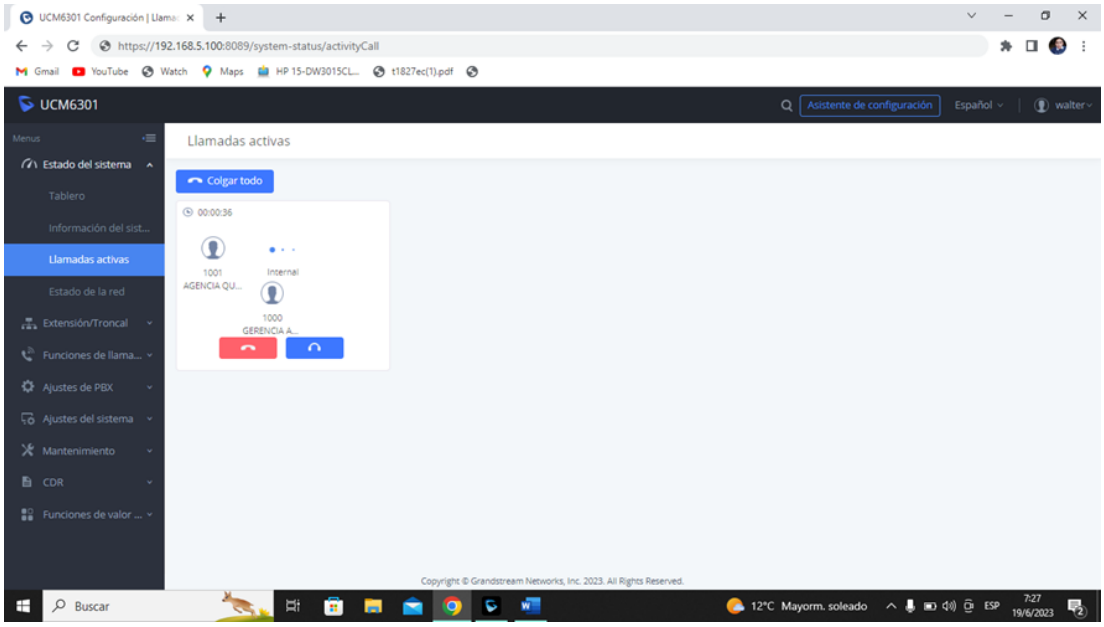


Figura 78. Funcionamiento correcto del sistema

Elaborado por: El Investigador

3.2.6 Pruebas de funcionamiento

Se llevaron a cabo pruebas directas en la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua, ya que la institución mantiene sus funciones operativas y continúa brindando servicios a sus usuarios. El objetivo de estas pruebas fue evaluar el rendimiento y la eficacia del sistema implementado en dicha Cooperativa.

El propósito de aplicar el sistema implementado fue observar su desarrollo en tiempo real y garantizar su eficacia en la Cooperativa. Por lo tanto, se realizaron pruebas específicas para verificar el acceso directo al sistema de videovigilancia desde la sala de monitoreo de la matriz central de control.

Durante estas pruebas, se evaluó la conexión y la funcionalidad del sistema para asegurarse de que tanto el DVR como el sistema de videovigilancia fueran accesibles en tiempo real. Esto permitió la visualización y el registro de información relevante relacionada con la seguridad y el monitoreo.

- **Prueba de acceso DVR y sistema de videovigilancia de la matriz**

Se llevó a cabo una prueba directa para acceder en tiempo real al DVR de la matriz y al sistema de videovigilancia desde la sala de monitoreo. En esta prueba, se comprobó los equipos instalados y funcionales como el DVR que permitió grabar y almacenar videos en tiempo real utilizando las cámaras de seguridad instaladas en la matriz proporcionando la visualización de los videos almacenados y mostrados en el servidor. La representación gráfica se encuentra en la figura 79, que muestra el acceso y funcionamiento de este sistema.

Figura 79. Ingreso al DVR y verificación de las cámaras desde la matriz

Elaborado por: El Investigador

- **Prueba de acceso a una sucursal desde la matriz**

En esta prueba de funcionamiento, se llevó a cabo un procedimiento similar, pero con el objetivo de verificar el monitoreo y control de una sucursal desde la matriz central. En este caso, se logró acceder con éxito al DVR de las cámaras de videovigilancia de la sucursal por medio del computador, y se pudo comprobar el monitoreo en tiempo real a través de la interfaz. Los resultados de esta prueba fueron exitosos, como se muestra en la figura 80.

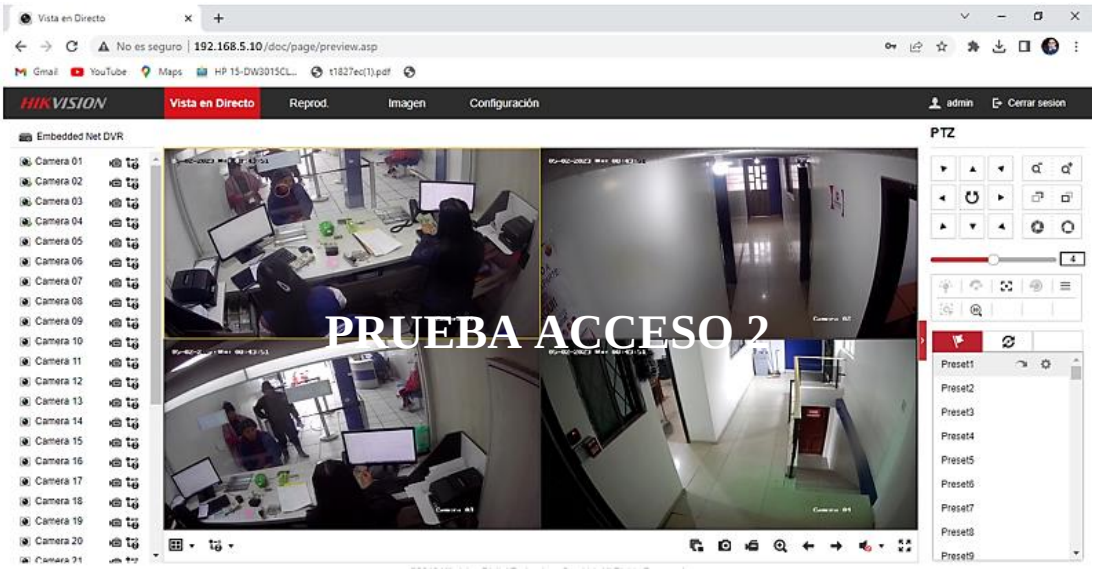


Figura 80. Ingreso a DVR de las cámaras de la sucursal desde la matriz

Elaborado por: El Investigador

- **Prueba de llamada Agencia-Gerencia**

Se lleva a cabo una prueba de llamada entre la Agencia Quisapincha y la central de Gerencia en Ambato para verificar el correcto funcionamiento de las extensiones asignadas. La figura 81 muestra que el funcionamiento es adecuado y sin problemas.

Figura 81. Prueba de llamada Agencia Quisapincha-Gerencia Ambato

Elaborado por: El Investigador

La prueba de llamada se ha realizado con éxito y una vez aceptada, se presentan múltiples opciones en la interfaz, como la capacidad de realizar llamadas directas, videollamadas y chatear con las diversas extensiones creadas. Además, después de

aceptar la llamada, existe la opción de compartir la pantalla. La figura 82 muestra una interacción exitosa con la interfaz.

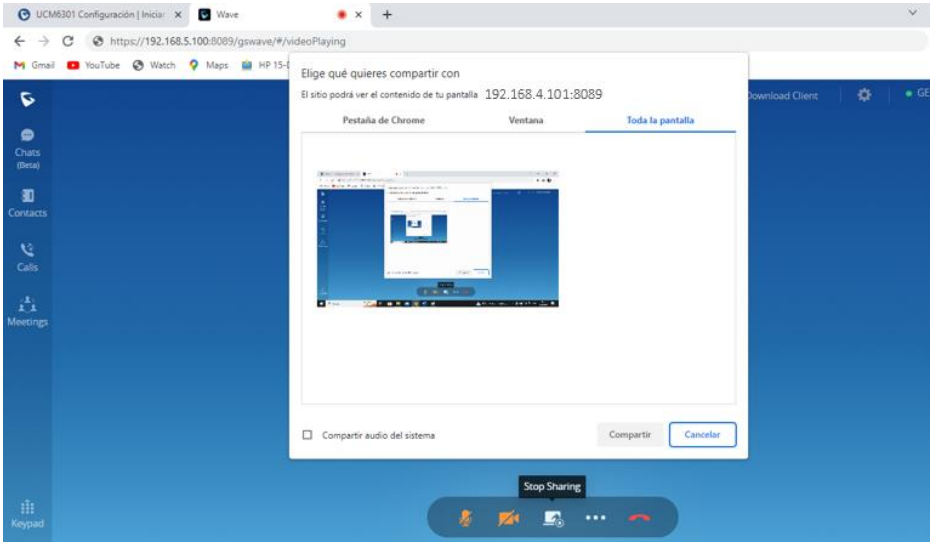


Figura 82. Interacción con la interfaz utilización exitosa de herramientas

Elaborado por: El Investigador

- **Prueba de llamada Gerencia Ambato-Gerencia Ambato 1000**

A través de la figura 83, se puede observar el estado exitoso de la conexión, confirmando que la comunicación entre las áreas Gerencia de Ambato y la Gerencia de Ambato (1000), se ha establecido correctamente garantizando la eficiencia y la calidad en las comunicaciones internas de la empresa

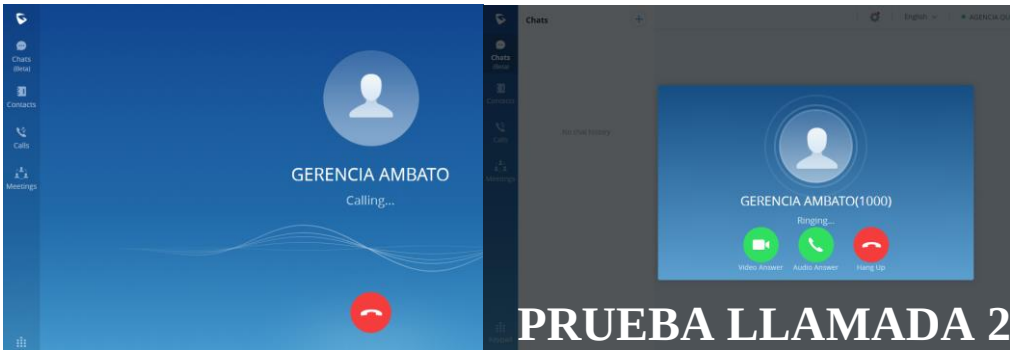


Figura 83. Prueba de llamada Gerencia Ambato-Gerencia Ambato 1000

Elaborado por: El Investigador

Al igual que otras plataformas de videoconferencia, GRANSTREM ofrece características y herramientas que permiten a los usuarios acceder y compartir su pantalla durante las sesiones. Estas funcionalidades son fundamentales para facilitar la colaboración y la presentación de información visual.

En la figura 84, se puede apreciar la prueba de estas funciones, lo cual proporciona una representación visual de cómo los usuarios pueden compartir su pantalla en la plataforma GRANSTREM. Esta herramienta permite a los participantes de la videoconferencia mostrar documentos, presentaciones, aplicaciones o cualquier contenido relevante directamente desde su pantalla.

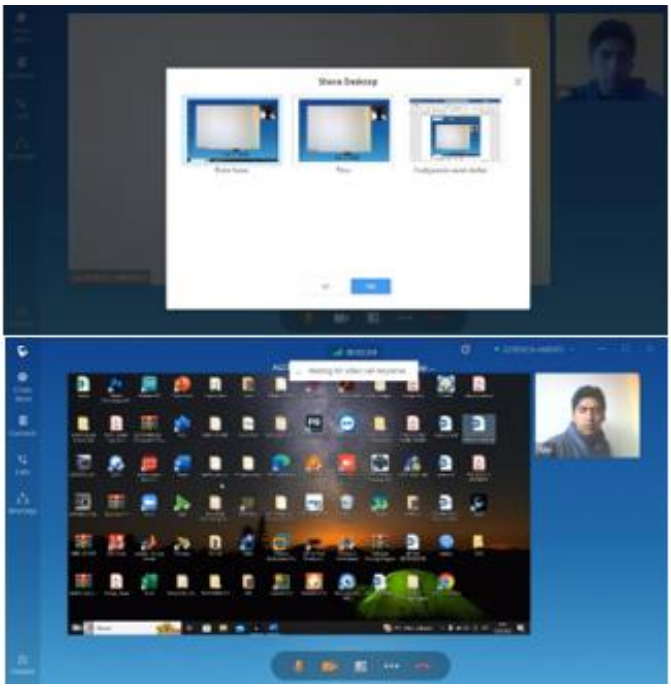


Figura 84. Interacción con la interfaz utilización exitosa de herramientas

Elaborado por: El Investigador

3.2.7 Integración de las sucursales de la Cooperativa De Ahorro Y Crédito Vencedores De Tungurahua En El Ecuador

Para realizar la integración de las sucursales y la matriz de la Cooperativa De Ahorro Y Crédito Vencedores De Tungurahua se realizaron los siguientes pasos como se detallan a continuación.

- Análisis actual de la red y dispositivos que dispone la cooperativa Cooperativa De Ahorro Y Crédito Vencedores. Como se detalla en la tabla 40.

Tabla 40. Análisis general y dispositivos de red Cooperativa Vencedores

Cooperativa vencedores	Router Mikrotik	Puertos de red disponible	Cámaras de video vigilancia	Telefonía IP	Mikrotik soporta VPN
Matriz Ambato	SI	NO	SI	SI	SI
Sucursal Quisapincha	SI	NO	SI	SI	SI
Sucursal Riobamba	SI	SI	SI	SI	SI
Sucursal Latacunga	SI	SI	SI	SI	SI
Sucursal Quito	SI	SI	SI	SI	SI
Sucursal Saquisili	SI	SI	SI	SI	SI

Elaborado por: El Investigador

- Identificación de la IP pública de cada una de las sucursales y la matriz, esto se puede visualizar en la tabla 41.

Tabla 41. Dirección IP publica Cooperativa Vencedores

	IP Pública
Matriz Ambato	200.24.139.2
Sucursal Quisapincha	186.3.45.138
Sucursal Riobamba	192.168.255.253
Sucursal Latacunga	172.20.18.150
Sucursal Quito	192.135.250.10
Sucursal Saquisili	192.31.7.11

Elaborado por: El Investigador

- Determinación protocolo de comunicación. En este caso se utilizó el protocolo UDP que permite trabajar con paquetes estandarizado RTP para el envío de

vídeo y audio a través de Internet. En la tabla 42, se detalla algunos protocolos utilizados para la transmisión de video IP.

Tabla 42. Análisis general y dispositivos de red Cooperativa Vencedores

Protocolo	Protocolo de transporte	Puerto	Uso o aplicación en la red
FTP	TCP	21	Transferencia de imágenes o vídeo desde una cámara de red a un servidor FTP o a una aplicación.
SMTP	TCP	25	Una cámara de red puede enviar imágenes o notificaciones de alarma utilizando su cliente integrado de e-mail.
HTTP	TCP	80	La transferencia de vídeo desde una cámara de red trabaja como un servidor web, proporcionando vídeo al usuario.
HTTPS	TCP	443	La transmisión de vídeo puede ser utilizada para autenticar los envíos de la cámara utilizando certificados digitales.
RTP	UDP/TCP	No definido	Formato de paquetes estandarizado RTP utilizado para el envió de video y audio a través de internet. Utilizado en sistema multimedia o video conferencia. La transferencia puede ser unicast o multicast.

Elaborado por: El Investigador

- Selección de equipos faltantes. En este caso al no disponer de puntos de red en el Mikrotik que posee la Cooperativa Vencedores tanto en la matriz como la sucursal Quisapincha, se adquirió el mikrotik RB2011UiAS-RB. Algunas de las características de este router se pueden ver en la tabla 39.
- Dimensionamiento de ancho de banda para la integración de servicios. Esto se puede ver en el punto 3.2.5.
- Por último, para la integración de las sucursales se realizó la programación de los diferentes router de cada sucursal, esto se puede ver en el apartado 3.2.3. En este apartado debido que es una institución financiera se coloca la información necesaria y supervisada por la Cooperativa de Ahorro y Crédito Vencedores de Tungurahua para evitar posibles ataques informáticos en un futuro.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

La Cooperativa de Ahorro y Crédito Vencedores de Tungurahua en la oficina matriz y sucursal Quisapincha, al ser las oficinas mas importantes y con mayor número de puntos de red al Router Mikrotik CRS326-24GZSTRM no dispone de puertos Ethernet, de manera que se procedió a la adquisición de dos router RB2011UiAS-RB, estos router cumplen con las características para establecer la comunicación VPNs y soportan el protocolo IPsec.

El sistema de comunicación VoIP, que posee la institución financiera es un sistema interno para cada oficina, el cual cuenta como servidor Grandstream UCM 6202-2, este servidor no soporta video llamadas, video conferencias. Para este caso se adquirió como servidor al Grandstream UCM 6301 que permite crea video llamadas, video conferencias, etc.

Para la implementación de la sala de monitoreo se estableció varios parámetros, tipo de cámaras, números de cámaras de cada sucursal, DVR compatibles, calidad de imagen, resolución, detección de movimiento, reconocimiento facial entre otros. En este caso todas las cámaras como el DVR pertenece a una misma marca como es

HIKVISION, permitiendo la configuración de forma más rápida y sencilla. Pero la mayoría de las cámaras son de características básicas es decir no tiene reconocimiento facial, lo que en un futuro se plantea el cambio de las cámaras para que el sistema de monitoreo trabaje de mejor manera.

En análisis de ancho de banda es muy importante para que el sistema funcione correctamente, en es este caso se debe analizar cada uno de los dispositivos que formen parte de la red de internet de cada oficina, En la actualidad los equipos de red de la Cooperativa Vencedores son de bajo consumo, debido a que tiene restricciones para navegar de forma libre por internet. Además, la cooperativa tiene contratado un ancho de banda de 25 a 30 Mbps en la mayoría de sus oficinas, de forma que al realizar los cálculos necesitamos un ancho de banda entre 11 a 15 Mbps para que nuestro sistema funcione correctamente.

La Cooperativa de Ahorro y Crédito Vencedores de Tungurahua con la implementación del sistema de comunicación y video vigilancia, permite reducir el riesgo de seguridad que enfrente la Cooperativa en cada una de sus sucursales.

4.2 Recomendaciones

Se recomienda llevar a cabo un análisis de expansión de la red en las sucursales de la Cooperativa, considerando la disponibilidad de servicios de Internet a través de fibra óptica. El objetivo de evaluar el aumento de velocidad o ancho de banda de Internet, para obtener una mayor velocidad de transmisión y mejorar la calidad de los servicios de videovigilancia y telefonía IP.

Se recomienda configurar las cámaras de videovigilancia con una detección de cinco imágenes por segundo, con el objetivo de garantizar la calidad y velocidad de transmisión de las imágenes, al mismo tiempo que se logra un ahorro de ancho de banda.

Se sugiere utilizar software de monitoreo de red para tener una visualización continua del progreso de la red, así como para ejecutar acciones correctivas en caso de problemas y asegurar el flujo de tráfico en los diferentes puntos o sucursales. Además, plantear los problemas con anticipación puede mejorar considerablemente la calidad del servicio de la red y del sistema en general.

Se sugiere asignar una dirección IP única a cada host para poder identificar de manera directa su ubicación física y lógica. Esta asignación facilita el manejo y tratamiento eficiente de cada terminal de usuario, permitiendo una respuesta más rápida y efectiva.

BIBLIOGRAFÍA

[1] L. Firdaouss, B. Ayoub, B. Manal, y Y. Ikrame, «Automated VPN configuration using DevOps», *Procedia Comput. Sci.*, vol. 198, pp. 632-637, 2022, doi: 10.1016/j.procs.2021.12.298.

[2] Patiño Tapia, Silvana Isabel, «Diseño e implementación de un enlace de radio para interconectar la oficina matriz de la Cooperativa Puéllaro y sus sucursales», Universidad Politecnica Salesiana, Quito, 2017. [En línea]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/14535

[3] David Herminio Castro Cuba Sayco, «Diseño e implementación de la interconexión de sucursales de HP-Store en las ciudades de Arequipa y Cusco mediante VPN con Mikrotik Routerboard», UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA, Arequipa, 2019. [En línea]. Disponible en: http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/8663/IEcsdh.pdf?sequence=1&isAllowed=y

[4] Miranda Quishpe, Jessica Daniela, «Sistema de comunicación en tiempo real con QOS para la integración de las unidades de salud de la provincia de Pastaza», Universidad Técnica de Ambato, Ambato, 2021. [En línea]. Disponible en: https://repositorio.uta.edu.ec/jspui/handle/123456789/33160

[5] O. D. Vega y S. Núñez, «Influencia del volumen de tráfico sobre túnel VPN IPSEC/UDP en enlaces WAN», *Télématique*, vol. 11, n.º 1, pp. 84-98, 2012.

[6] S. M. C. Delgado, «Revisión sistemática de Comunicaciones Unificadas de VoIP en redes CAN», *Informática Sist. Rev. Tecnol. Informática Las Comun.*, vol. 5, n.º 1, Art. n.º 1, sep. 2021, doi: 10.33936/isrtic.v5i1.3569.

[7] A. Alharbi, A. Bahnasse, y M. Talea, «A Comparison of VoIP Performance Evaluation on different environments Over VPN Multipoint Network», *Int. J. Comput. Sci. Netw. Secur.*, vol. 17, pp. 123-128, may 2017.

[8] M. Velasquez y V. Ronald, «Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764», *Univ. Peru. Cienc. Apl. UPC*, abr. 2019, doi: 10.19083/tesis/625693.

[9] «Reseña Historica – Coac Vencedores – Tu confianza firme». https://www.coacvencedores.com/historia/ (accedido 7 de marzo de 2023).

[10] «Redes de comunicaciones». https://www.monografias.com/trabajos-pdf2/redes-comunicaciones/redes-comunicaciones (accedido 7 de marzo de 2023).

[11] «Concepto Social Del Esquema De La Red De Comunicación Ilustración del Vector - Ilustración de medio, grupo: 62449447». https://es.dreamstime.com/stock-de-ilustración-concepto-social-del-esquema-de-la-red-de-comunicación-image62449447 (accedido 7 de marzo de 2023).

[12] «Parametros que definen una red | Guías, Proyectos, Investigaciones de Telecomunicación | Docsity». https://www.docsity.com/es/parametros-que-definen-una-red/5474546/ (accedido 7 de marzo de 2023).

[13] «Topología de red: qué es y cuáles son los tipos más habituales | UNIR Ecuador». https://ecuador.unir.net/actualidad-unir/topologia-red/ (accedido 7 de marzo de 2023).

[14] B. Noguera, «Topología de red: malla, estrella, árbol, bus y anillo», *Culturación*, 13 de noviembre de 2014. https://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/ (accedido 7 de marzo de 2023).

[15] «Topología de redes: Infraestructura básica de una red», *Blog de InGenio Learning*, 23 de abril de 2021. https://ingenio.edu.pe/blog/topologia-de-redes-infraestructura-basica-de-una-red/ (accedido 7 de marzo de 2023).

[16] «Topología de anillo: características, ventajas, desventajas», *Lifeder*, 9 de octubre de 2019. https://www.lifeder.com/topologia-de-anillo/ (accedido 7 de marzo de 2023).

[17] «¿Qué es Topología de red de malla (red de malla)? - Definición en WhatIs.com», *ComputerWeekly.es*. https://www.computerweekly.com/es/definicion/Topologia-de-red-de-malla-red-de-malla (accedido 7 de marzo de 2023).

[18] «Topologia de árbol», *Redes Inalambricas y Cableadas.*, 22 de octubre de 2014. https://redesinalambricasycableadas.wordpress.com/redes-cableadas/diferentes-topologias-de-red/topologia-de-arbol/ (accedido 7 de marzo de 2023).

[19] «¿Cuáles son los tipos de redes de computadoras?» http://worldcampus.saintleo.edu/noticias/cuales-son-los-tipos-de-redes-de-computadoras (accedido 7 de marzo de 2023).

[20] «Cuáles son los principales servicios de red», *OpenWebinars.net*, 16 de marzo de 2020. https://openwebinars.net/blog/cuales-son-los-principales-servicios-de-red/ (accedido 7 de marzo de 2023).

[21] S. Hernández, «【 Servicios de Red 】¿Qué Son? + ¿Qué Tipos Existen? ▷ 2023», *Internet Paso a Paso*, 24 de octubre de 2019. https://internetpasoapaso.com/servicio-de-red/ (accedido 7 de marzo de 2023).

[22] «Protocolo de red: Qué es, tipos y características», *OpenWebinars.net*, 17 de septiembre de 2021. https://openwebinars.net/blog/protocolo-de-red-que-es-tipos-y-caracteristicas/ (accedido 7 de marzo de 2023).

[23] «¿Qué es el enrutamiento? | Enrutamiento IP», *Cloudflare*. https://www.cloudflare.com/es-es/learning/network-layer/what-is-routing/ (accedido 8 de marzo de 2023).

[24] A. Walton, «Enrutamiento Estático y Dinámico » CCNA desde Cero», *CCNA desde Cero*, 23 de junio de 2020. https://ccnadesdecero.es/enrutamiento-estatico-y-dinamico/ (accedido 8 de marzo de 2023).

[25] «¿Qué es un túnel VPN? - Tech Advisor». https://www.techadvisor.com/article/1407571/que-es-un-tunel-vpn.html (accedido 8 de marzo de 2023).

[26] M. G. Soto, «Entendiendo los túneles…», *Medium*, 8 de junio de 2016. https://marvin-soto.medium.com/entendimiento-los-t%C3%BAneles-ecd7a6a80634 (accedido 8 de marzo de 2023).

[27] «Las principales ventajas y desventajas de una VPN – Resumen - Shellfire Blog». https://www.shellfire.es/blog/vpn-ventajas-y-desventajas/ (accedido 8 de marzo de 2023).

[28] «Conoce los tipos de VPN y sus protocolos». https://www.kionetworks.com/blog/data-center/tipos-de-vpn-y-sus-protocolos (accedido 8 de marzo de 2023).

[29] «Comunicaciones seguras utilizando SSL (Secure Sockets Layer - Capa de sockets seguros) - Documentación de IBM». https://www.ibm.com/docs/es/was-nd/9.0.5?topic=communications-secure-using-ssl (accedido 8 de marzo de 2023).

[30] «IBM Documentation», 13 de diciembre de 2022. https://www.ibm.com/docs/es/was-nd/9.0.5?topic=communications-secure-using-ssl (accedido 8 de marzo de 2023).

[31] «¿Qué es OpenVPN? | Servicio al cliente de NordVPN». https://support.nordvpn.com/es/Informaci%C3%B3n-general/1821135152/-Qu%C3%A9-es-OpenVPN.htm (accedido 8 de marzo de 2023).

[32] «Opciones de Calidad de Servicio en Interfaces de Túnel GRE - Cisco». https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/10106-qos-tunnel.html (accedido 8 de marzo de 2023).

[33] AlvaroM, «Protocolo UDP - User Datagram Protocol», *Networkgeeks*, 4 de diciembre de 2018. https://netwgeeks.com/udp-user-datagram-protocol/ (accedido 8 de marzo de 2023).

[34] C. A. García, E. X. Castellanos, y M. V. García, «UML-Based Cyber-Physical Production Systems on Low-Cost Devices under IEC-61499», *Machines*, vol. 6, n.º 2, Art. n.º 2, jun. 2018, doi: 10.3390/machines6020022.

[35] «4diac FORTE - El entorno de ejecución de 4diac». https://www.eclipse.org/4diac/en_rte.php (accedido 27 de diciembre de 2022).

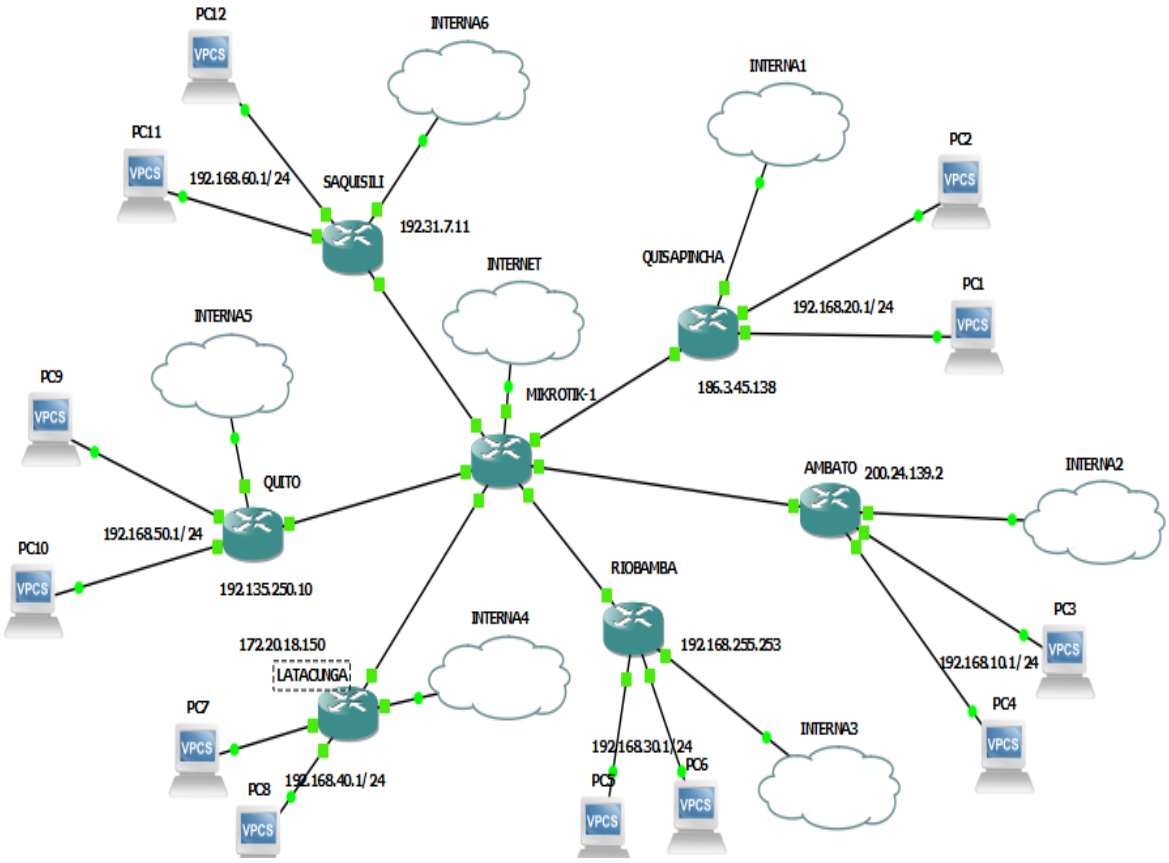
[36] Enzyme, «Redes neuronales con Python: ¿por qué es el mejor lenguaje para IA?» https://enzyme.biz/blog/redes-neuronales-python (accedido 27 de diciembre de 2022).

[37] K. S. Narendra y K. Parthasarathy, «Gradient methods for the optimization of dynamical systems containing neural networks», *IEEE Trans. Neural Netw.*, vol. 2, n.º 2, pp. 252-262, mar. 1991, doi: 10.1109/72.80336.

ANEXOS

ANEXO A

RED PROPUESTA PARA LA COOPERATIVA DE AHORRO Y CREDITO VENCEDORES DE TUNGURAHIA



ANEXO B

PROGRAMACIÓN VPN OFICINA MATRIZ - SUCURSAL RIOBAMBA

Router Matriz Ambato

/ip ipsec peer

add address=200.24.139.2 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.10.0/24

dst-address=192.168.30.0/24 sa-src-address=192.168.255.253

sa-dst-address=200.24.139.2 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.10.0/24

dst-address=192.168.30.0/24 place-before=0

/ip ipsec proposal

Router Sucursal Riobamba

/ip ipsec peer

add address=192.168.255.253 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.30.0/24

dst-address=192.168.10.0/24 sa-src-address=200.24.139.2

sa-dst-address=192.168.255.253 tunnel=yes

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.30.0/24

dst-address=192.168.10.0/24 place-before=0

ANEXO C

PROGRAMACIÓN VPN OFICINA MATRIZ - SUCURSAL QUISAPINHA

Router Matriz Ambato

/ip ipsec peer

add address=200.24.139.2 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.10.0/24

dst-address=192.168.20.0/24 sa-src-address=186.3.45.138

sa-dst-address=200.24.139.2 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.10.0/24

dst-address=192.168.20.0/24 place-before=0

Router Sucursal Quisapincha

/ip ipsec peer

add address=186.3.45.138 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.20.0/24

dst-address=192.168.10.0/24 sa-src-address=200.24.139.2

sa-dst-address=186.3.45.138 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.20.0/24

dst-address=192.168.10.0/24 place-before=0

ANEXO D

PROGRAMACIÓN VPN OFICINA MATRIZ - SUCURSAL SAQUISILI

Router Matriz Ambato

/ip ipsec peer

add address=200.24.139.2 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.10.0/24

dst-address=192.168.60.0/24 sa-src-address=192.31.7.11

sa-dst-address=200.24.139.2 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.10.0/24

dst-address=192.168.60.0/24 place-before=0

Router Sucursal Saquisili

/ip ipsec peer

add address=192.31.7.11 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.60.0/24

dst-address=192.168.10.0/24 sa-src-address=200.24.139.2

sa-dst-address=192.31.7.11 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.60.0/24

dst-address=192.168.10.0/24 place-before=0

ANEXO E

PROGRAMACIÓN VPN OFICINA MATRIZ - SUCURSAL LATACUNGA

Router Matriz Ambato

/ip ipsec peer

add address=200.24.139.2 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.10.0/24

dst-address=192.168.40.0/24 sa-src-address=172.20.18.150

sa-dst-address=200.24.139.2 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.10.0/24

dst-address=192.168.40.0/24 place-before=0

Router Sucursal Latacunga

/ip ipsec peer

add address=172.20.18.150 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.40.0/24

dst-address=192.168.10.0/24 sa-src-address=200.24.139.2

sa-dst-address=172.20.18.150 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.40.0/24

dst-address=192.168.10.0/24 place-before=0

ANEXO F

PROGRAMACIÓN VPN OFICINA MATRIZ - SUCURSAL QUITO

Router Matriz Ambato

/ip ipsec peer

add address= 200.24.139.2 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.10.0/24

dst-address=192.168.50.0/24 sa-src-address=192.135.250.10

sa-dst-address= 200.24.139.2 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.10.0/24

dst-address=192.168.50.0/24 place-before=0

Router Sucursal Quito

/ip ipsec peer

add address=192.135.250.10 secret=“ipsec-pass” port=500

auth-method=pre-shared-key

/ip ipsec policy

add proposal="ipsec" src-address=192.168.50.0/24

dst-address=192.168.10.0/24 sa-src-address=200.24.139.2

sa-dst-address=192.135.250.10 tunnel=yes

/ip ipsec proposal

add name="ipsec" auth-algorithms=sha1 enc-algorithms=3des lifetime=30m pfs-group=modp1024

/ip firewall nat

add action=accept chain=srcnat src-address=192.168.50.0/24

dst-address=192.168.10.0/24 place-before=0

ANEXO G

CATÁLOGO ROUTER MIKROTIK RB2011UIAS-RM

RB2011 Series

RB2011 are multifunctional routers with 5 Gigabit Ethernet ports and 5 Fast Ethernet ports, and multiple models available. The RB2011iL are lower cost, but the RB2011Ui series have full features.

All RB2011 devices are powered by a new generation Atheros 600MHz 74K MIPS CPU.

Model	RB2011iL	RB2011UiAS
CPU	Atheros AR9344 600MHz	
Memory	64MB DDR SDRAM onboard memory	128MB DDR SDRAM onboard memory
Ethernet	Five 10/100 Mbit Fast Ethernet ports with Auto-MDI/X Five 10/100/1000 Mbit Gigabit Ethernet ports with Auto-MDI/X	
Extras	Reset button, Reset jumper	
LEDs	Power, User, Ethernet activity	
Power input	Jack 8-28V DC; PoE in: 8-28V DC on Ether1 (Non 802.3af).	
Power output	500mA on Port 10	
Dimensions	Desktop:230x90x25mm Rackmount:443x92x44mm	
Power consumption	8W max	15W max
Operating System	MikroTik RouterOS, L4 license	MikroTik RouterOS, L5 license
Package includes	RB2011, power supply	

Feature / Model	2011iL-IN	2011iL-RM	2011iLS-IN	2011UiAS-IN	2011UiAS-RM
Enclosure	Desktop	Rackmount	Desktop	Desktop	Rackmount
SFP port	-	-	Yes	Yes	Yes
Power output	on port 10	on port 10	on port 10	on port 10	on port 10
USB	-	-	-	Yes	Yes

ANEXO H

CATÁLOGO GRANDSTREAM UCM 6301

Solución de Comunicación Unificada para Empresas

Serie UCM6300

La serie UCM6300 permite a los negocios crear poderosas y expansibles soluciones de comunicaciones unificadas y colaboración. Esta serie de IP PBXs proporciona una plataforma que unifica todas las comunicaciones empresariales en una red centralizada, incluyendo voz, videollamadas, videoconferencias, videovigilancia, reuniones web, datos, análisis, movilidad, acceso a instalaciones, intercomunicadores y más. La serie UCM6300 admite hasta 3,000 usuarios e incluye una solución integrada de reuniones web y videoconferencias que permite a los empleados conectarse desde los dispositivos y teléfonos IP móviles y de escritorio de la serie GVC. Puede acompañarse con el ecosistema UCM6300 para ofrecer una plataforma híbrida que combine el control de un IP PBX en sitio con el acceso remoto de una solución en la nube. El ecosistema UCM6300 consiste en la aplicación Wave para dispositivos de escritorio web y móviles, la cual proporciona un punto central para colaborar a distancia, y en UCM RemoteConnect, un servicio NAT Traversal en la nube para garantizar conexiones remotas seguras. La serie UCM6300 también ofrece configuración y gestión en la nube a través de GDMS y una API para integración con plataformas de terceros. Al ofrecer una sofisticada solución de comunicaciones unificadas y colaboración equipada con un conjunto de herramientas de movilidad, seguridad, reunión y colaboración, la serie UCM6300 proporciona una poderosa plataforma para cualquier organización.

3000 users

Permite hasta 3000 usuarios y hasta 450 llamadas simultáneas

zero CONFIG

Aprovisionamiento Zero-Config de dispositivos SIP Grandstream

Plataforma integrada de conferencias y reuniones; soporta terminales de escritorio, dispositivos SIP y la aplicación Wave

La app Wave permite la comunicación con todos los usuarios y las soluciones UCM6300

API

API disponible para integraciones con terceros, incluyendo plataformas de CRM y PMS

Protección de seguridad avanzada con arranque seguro, certificado único y contraseña predeterminada aleatoria para proteger llamadas y cuentas

Gigabit

Tres puertos de red Gigabit RJ45 con detección automática con PoE+ integrado y modo Support NAT Router

UCM RemoteConnect

El servicio automatizado NAT Firewall Traversal facilita las conexiones remotas seguras

Mayor confiabilidad con soporte para el modo Hot Standby High Availability

HD

Soporta códec de voz Full-Band Opus y códec de video H.264/ H.263/H.263+/VP8, resistencia a la fluctuación de hasta 50% de pérdida de paquetes

Compatible con GDMS para configuración, gestión y monitoreo en la nube

Basado en el sistema operativo de telefonía de fuente abierta Asterisk® versión 16

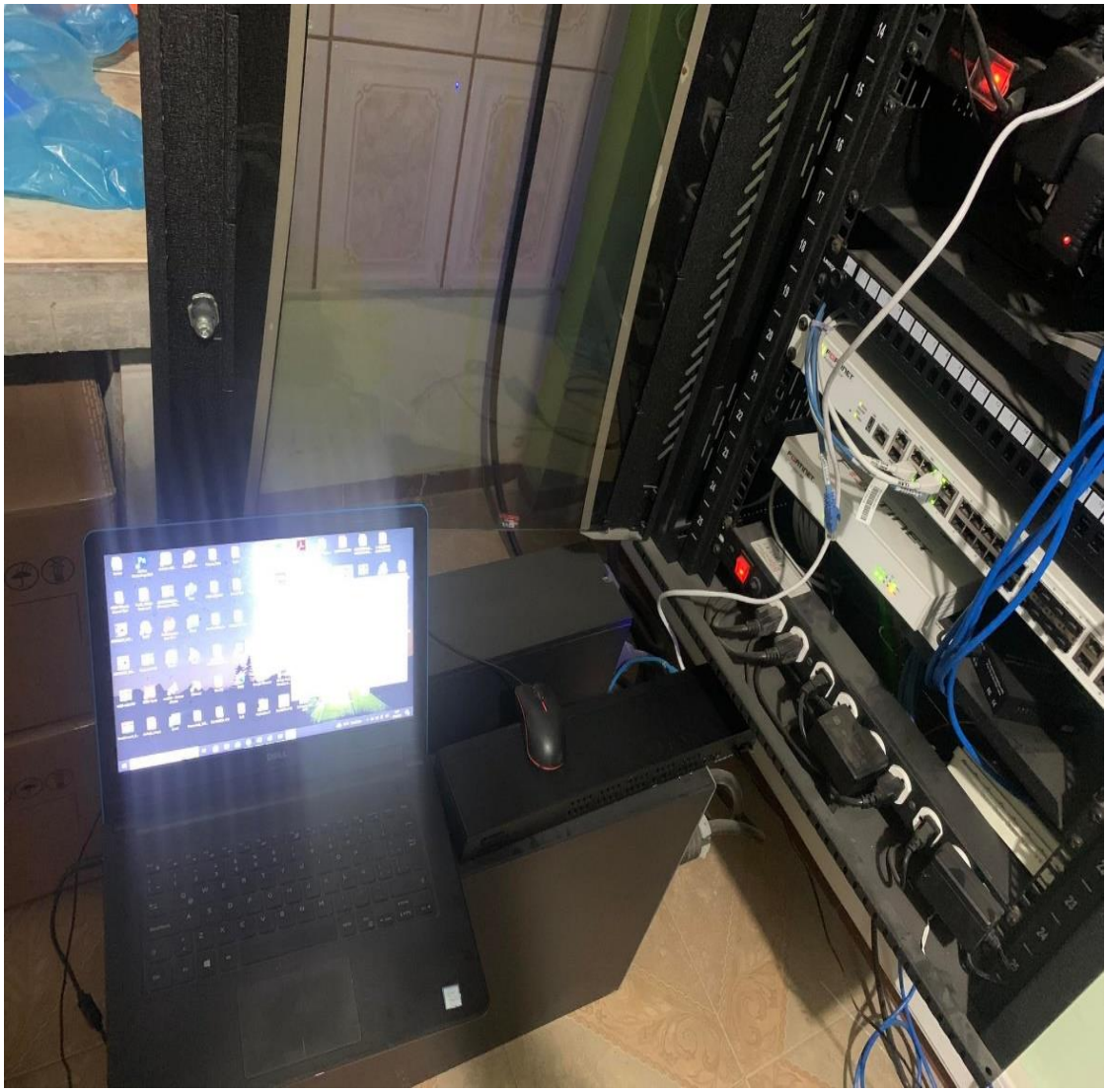
	UCM6301	UCM6302	UCM6304	UCM6308
Puertos FXS para Teléfono Analógico	1 Puerto RJ11	2 Puertos RJ11	4 Puertos RJ11	8 Puertos RJ11
	Todos los puertos tienen la funcionalidad de línea de emergencia en caso de falla eléctrica			
Puertos FXO para Línea PSTN	1 Puerto RJ11	2 Puertos RJ11	4 Puertos RJ11	8 Puertos RJ11
	Todos los puertos tienen la funcionalidad de línea de emergencia en caso de falla eléctrica			
Interfaces de Red	Tres puertos Gigabit autoadaptativos (conmutados, enrutados o en modo de tarjeta dual) con PoE+			
NAT Router	Sí (soporta modo enrutado y modo conmutado)			
Puertos Periféricos	1 Puerto USB 3.0, 1 interfaz de tarjeta SD	1 Puerto USB 2.0, 1 puerto USB 3.0, 1 interfaz de tarjeta SD	2 Puertos USB 3.0, 1 interfaz de tarjeta SD	
Indicadores LED	Ninguno		Power 1/2, FXS, FXO, LAN, WAN, Heartbeat	
Pantalla LCD	Pantalla táctil LCD a color de 320x240 para atajos de teclado y barra de desplazamiento		Pantalla gráfica LCD de matriz de puntos de 128x32 con botones DOWN y OK	
Interruptor de Reinicio	Sí, pulsación larga para restablecimiento de fábrica y pulsación corta para reinicio			
Capacidad de Voz por Paquetes	LEC con Unidad de Protocolo de Voz Paquetizada NLP, Cancelación de Eco de Línea de 128 ms de longitud de cola, Búfer Dinámico de Fluctuación (Jitter), detección de módem y conmutación automática a G.711, NetEQ, FEC 2.0, resistencia a la fluctuación de hasta 50% de pérdida de paquetes de audio			
Códecs de Voz y Fax	Opus, G.711 A-law/U-law, G.722, G722.1, G722.1C, G.723.1 5.3K/6.3K, G.726-32, G.729A/B, iLBC, GSM; T.38			
Códecs de Video	H.264, H.263, H263+, VP8			
QoS	Layer 2 QoS (802.1Q, 802.1p) y Layer 3 (ToS, DiffServ, MPLS) QoS			
API	API completa disponible para la integración de plataformas y aplicaciones de terceros			
Sistema Operativo de Telefonía	Basado en Asterisk versión 16			
Métodos DTMF	Audio en banda, RFC2833 y SIP INFO			
Protocolo de Aprovisionamiento y Tecnología Plug-and-Play	Aprovisionamiento masivo usando archivo de configuración XML cifrado con AES, autodetección y aprovisionamiento automático de dispositivos IP Grandstream por medio de ZeroConfig (DHCP Option 66 multicast SIP SUBSCRIBE mDNS), lista de eventos entre troncales locales y remotas			
Protocolos de Red	SIP, TCP/UDP/IP, RTP/RTCP, IAX, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay (en trámite), IPv6, OpenVPN®			
Métodos de Desconexión	Busy/Congestion/Howl Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect			
Cifrado de Medios	SRTP, TLS, HTTPS, SSH, 802.1X			
Fuente de Alimentación Universal	Entrada: 100 ~ 240VAC, 50/60Hz; Salida: DC 12V, 1.5A		2 Conectores de alimentación DC 12V Entrada: 100 ~ 240VAC, 50/60Hz; Salida: DC 12V, 2A	
Dimensiones	270 mm (longitud) x 175 mm (ancho) x 36 mm (altura)		485 mm (longitud) x 187.2 mm (ancho) x 46.2 mm (altura)	
Peso	Peso de Unidad: 715 g; Peso de Paquete: 1211 g	Peso de Unidad: 725 g; Peso de Paquete: 1221 g	Peso de Unidad: 2490 g; Peso de Paquete: 3260 g	Peso de Unidad: 2550 g; Peso de Paquete: 3320 g
Temperatura y Humedad	En operación: 32 ~ 113 °F / 0 ~ 45 °C, Humedad 10 - 90% (sin condensación) En almacenamiento: 14 ~ 140 °F / -10 ~ 60 °C, Humedad 10 - 90% (sin condensación)			
Montaje	Montaje en pared y escritorio		Montaje en rack y escritorio	
Soporte en Múltiples Idiomas	• Interfaz de Usuario Web: Inglés, Chino Simplificado, Chino Tradicional, Español, Francés, Portugués, Alemán, Ruso, Italiano, Polaco, Checo, Turco • IVR/indicaciones de voz personalizables: Inglés, Chino, Inglés Británico, Alemán, Español, Griego, Francés, Italiano, Holandés, Polaco, Portugués, Ruso, Sueco, Turco, Hebreo, Árabe, Neerlandés • Paquete personalizable de idiomas para permitir cualquier otro idioma			
Identificador de Llamadas	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 - BT, NTT			

ANEXO I

FOTOGRAFÍAS DEL PROTOTIPO IMPLEMENTADO

SUCURSAL PRINCIPAL QUISAPINCHA

En la siguiente imagen su puede observar el rack con los equipos que posee la sucursal de Quisapincha. Además, se puede ver el router adquirido RB2011UiAS-RB para la implementación del prototipo.

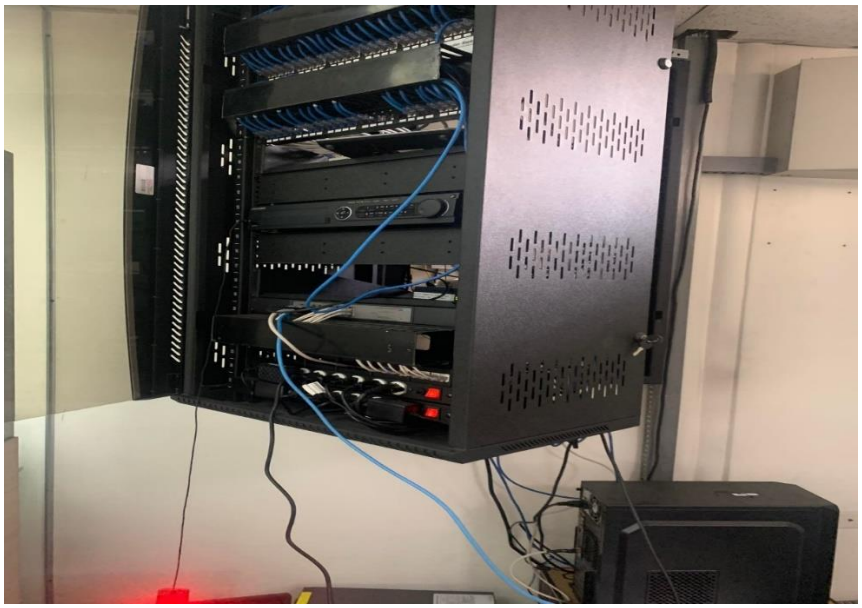


ANEXO J

FOTOGRAFÍAS DEL PROTOTIPO IMPLEMENTADO

SUCURSAL PRINCIPAL AMBATO

En la siguiente imagen se pude observar el rack de la matriz Ambato con sus respectivos dispositivos que posee.

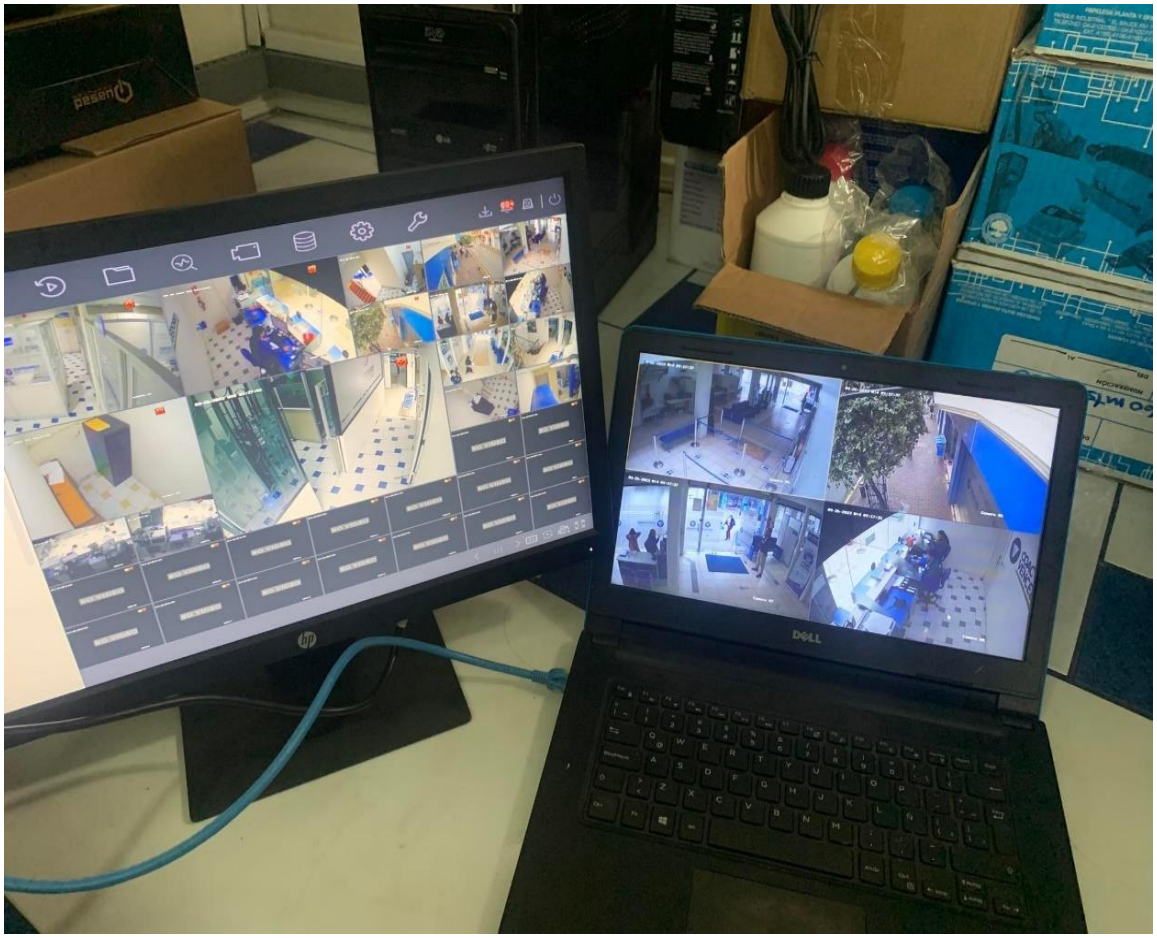


En la siguiente imagen se puede ver el router adquirido RB2011UiAS-RB para la implementación del prototipo en la matriz Ambato.

ANEXO K

FOTOGRAFÍAS PROTOTIPO SALA DE MONITOREO

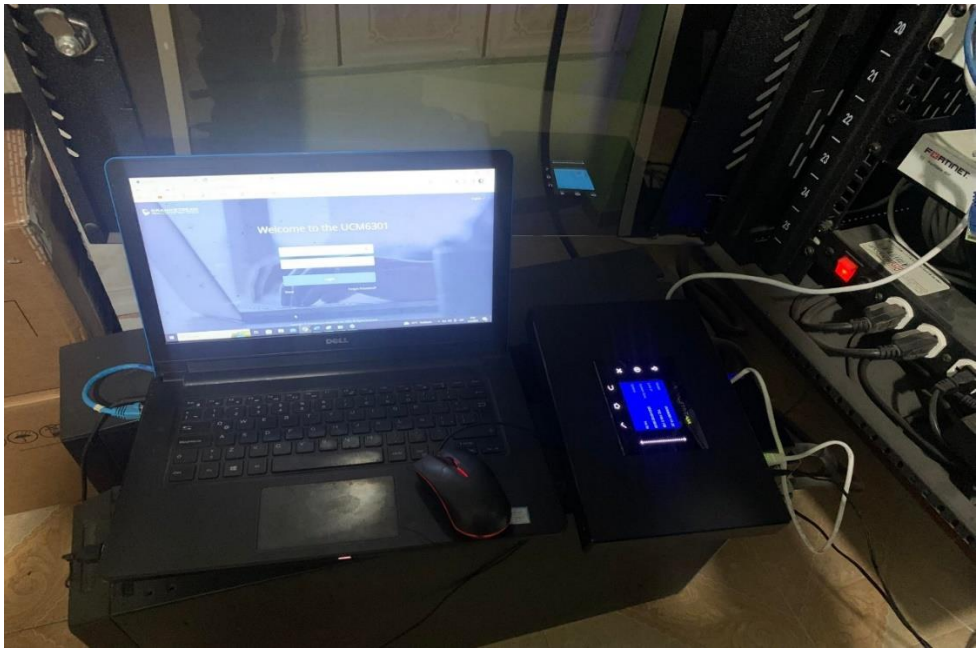
En la siguiente imagen se puede observar la sala de monitoreo implementado, como podemos ver tenemos acceso a las cámaras de video vigilancia de la matriz y sucursal quisapincha.



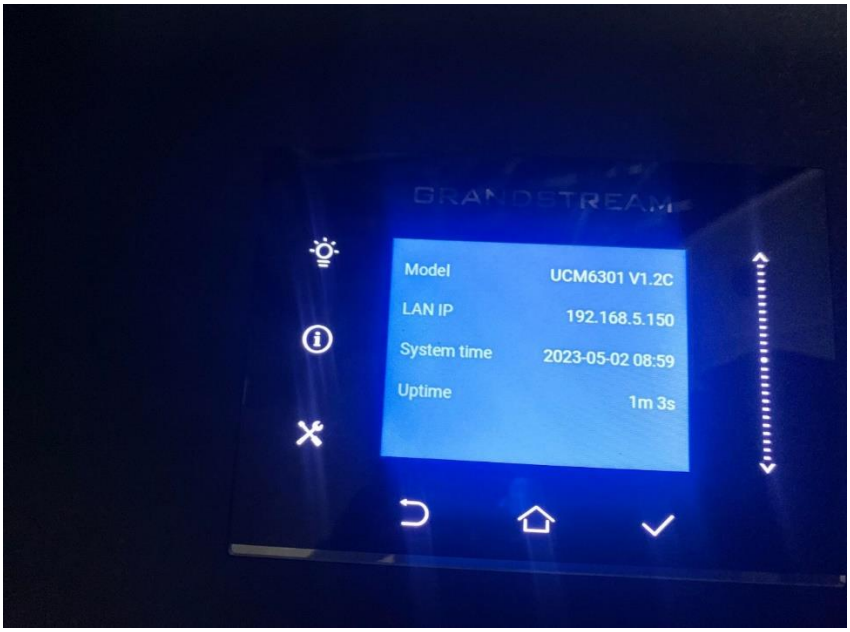
ANEXO L

FOTOGRAFÍAS IMPLEMENTACIÓN CENTRAL UCM6301

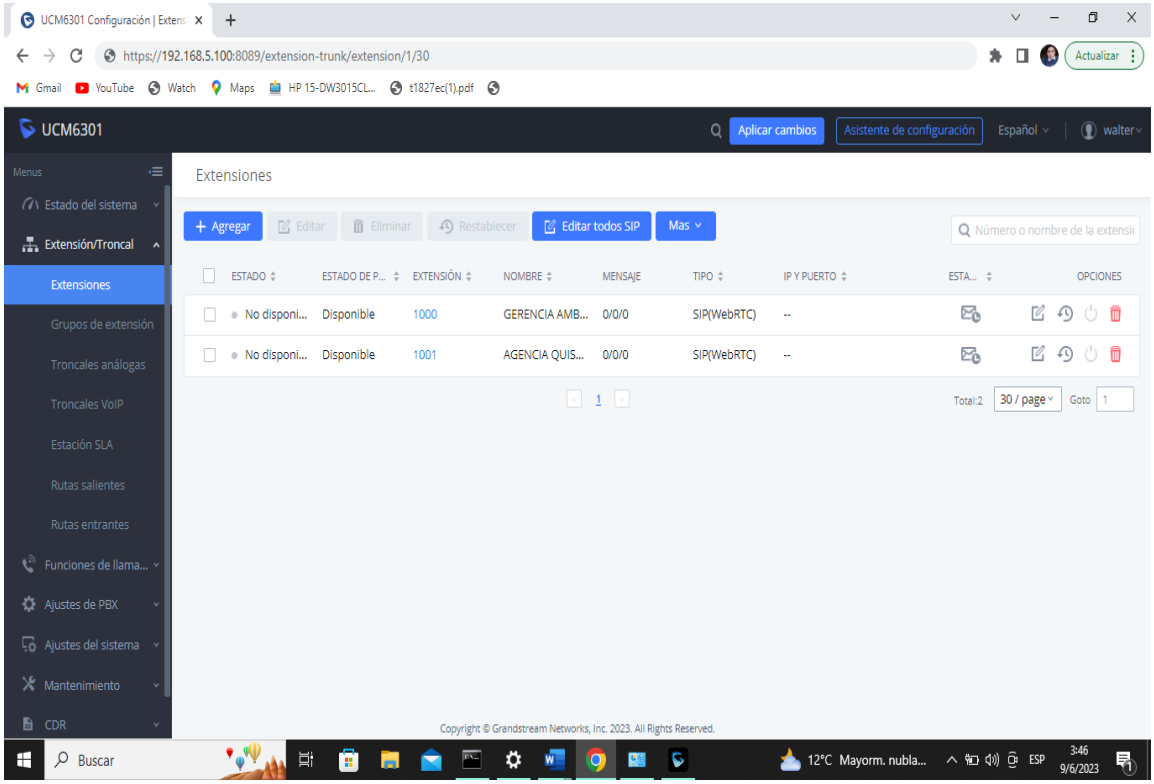
En la siguiente imagen se puede observar la configuración de la central telefónica UCM 6301. Donde desde el computador ingresamos a la interfaz de la programación.



En la siguiente imagen se puede observar los parámetros establecidos para la central telefónica UCM 6301.



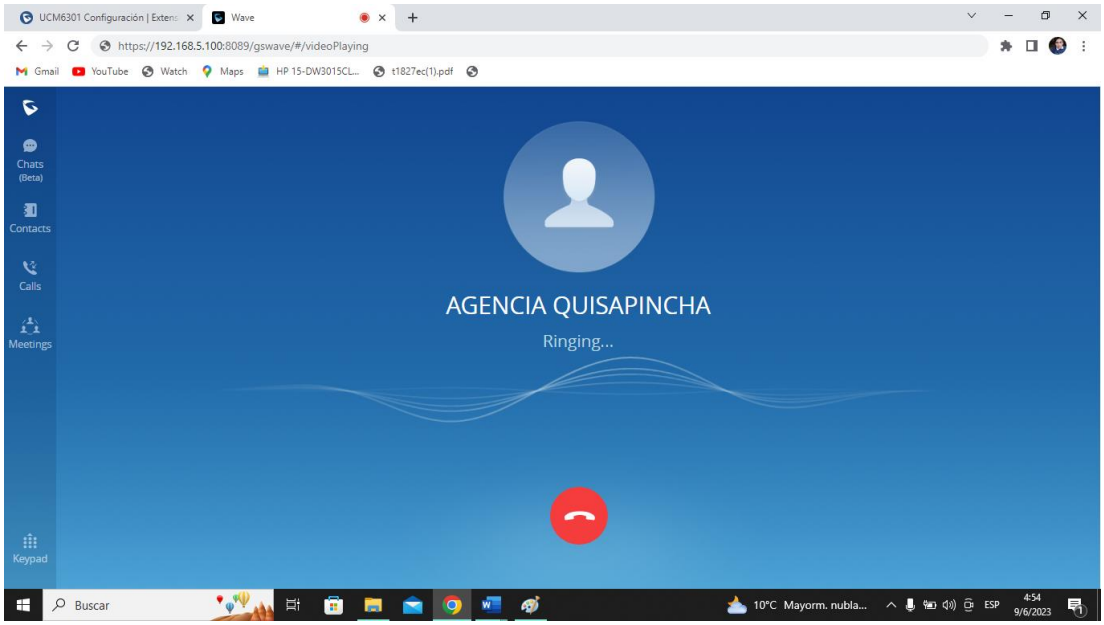
En la siguiente imagen se puede observar las extension creadas en la central telefonica tanto para la matriz de Ambato como para la sucursal de Quisapincha.



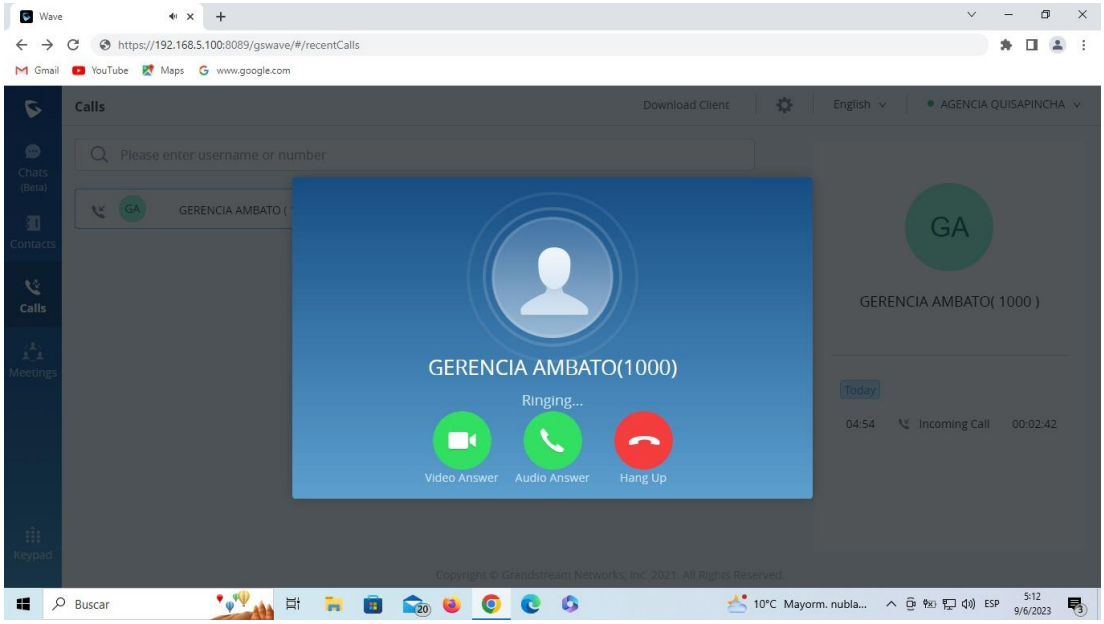
ANEXO M

PRUEBA DE FUNCIONAMINETO CENTRAL TELEFONICA

En la siguiente imagen se puede observar el funcionamiento de la central telefónica con las extensiones establecidas para lo cual se realiza una llamada desde la sucursal Quisapincha hacia la matriz Ambato.



En la siguiente imagen se puede observar que al realizar la llamada el teléfono estable comunicación con la matriz Ambato.



En la siguiente imagen se puede observar que al contestar la llamada se establece comunicación creado video llamadas lo cual permite la aplicación diferentes funciones como compartir pantallas agregar a la llamada a mas personas.